Available online at www.sciencedirect.com

ScienceDirect

Information and Computation 205 (2007) 624–650

Information and Computation

www.elsevier.com/locate/ic

Permutative rewriting and unification☆

Thierry Boy de la Tour *, Mnacho Echenim

LEIBNIZ laboratory, IMAG - CNRS INPG, 46 avenue Félix Viallet, F-38031 Grenoble Cedex, France

Received 9 September 2005; revised 29 September 2006
Available online 25 January 2007

Abstract

Permutative rewriting provides a way of analyzing deduction modulo a theory defined by leaf-permutative equations. Our analysis naturally leads to the definition of the class of *unify-stable* axiom sets, in order to enforce a simple reduction strategy. We then give a uniform unification algorithm modulo theories E axiomatized this way. We prove that it computes complete sets of unifiers of simply exponential cardinality, and that the E-unification decision problem belongs to **NP**.

Keywords: Equational theories; Term rewriting; E-unification; Permutation groups

1. Introduction

Unification, or the task of solving equations, is among the fundamental tools of Automated Reasoning. In *equational unification*, equations must be solved modulo a theory given by a set E of equational axioms. This is especially useful when E does not lead to a terminating rewrite relation, as in the well-studied theories C (commutativity, see [4]) and AC (C + associativity, see [21,9,10]). By contrast with the general case, C and AC-unification are decidable and *finitary*, i.e. any equation admits a finite set of minimal solutions w.r.t. subsumption.

☆ This work has been supported by CNRS and MENRT.
* Corresponding author. Fax: +33 4 76 57 50 81.
E-mail addresses: Thierry.Boy-de-la-Tour@imag.fr (T. Boy de la Tour), M.Echenim@imag.fr (M. Echenim).

0890-5401/$ - see front matter © 2006 Elsevier Inc. All rights reserved.
doi:10.1016/j.ic.2006.11.001

This raises the problem of extending such results to *classes* of theories containing C or AC. In [20] Schmidt-Schauß considered the class of *permutative* theories (defined by axioms $s \approx t$ where t can be obtained from s by permuting occurrences of symbols), and proved the undecidability of unification in one such theory. This result was later extended in [17] to the smaller class of *variable-permuting* theories (where only occurrences of variables may be permuted). The even smaller class of *leaf-permutative* theories is obtained by restricting the terms in the axioms to be linear. The decidability status of leaf-permutative unification is not known, while the existence of infinitary problems, questioned in [14], has been established in [19], by considering a theory defined by two axioms involving two function symbols. In [15], a similar result was proved with a leaf-permutative theory defined by a single axiom with a single function symbol, namely

$$f(f(x_1,x_2),f(x_3,x_4)) \approx f(f(x_1,x_3),f(x_2,x_4)).$$

Actually, we can exhibit an infinitary unification problem with an even simpler axiom: $f(f(x,y),z) \approx f(f(y,x),z)$. If we call $C1$ this theory (the arguments of an occurrence of f commute when it appears as the first argument of another occurrence of f) and consider the unification problem $f(x,z) =^{?}_{C1} f(y,z)$, it is easy to see that

$$\theta_n = \begin{cases} x \leftarrow f(x_1, f(\ldots, f(x_n, f(u,v))\ldots)) \\ y \leftarrow f(x_1, f(\ldots, f(x_n, f(v,u))\ldots)) \end{cases}$$

is a $C1$-unifier of our problem; the fact that $x\theta_n$ occurs as first argument of f in $f(x,z)\theta_n$ triggers a cascade of commutations, down to $f(f(u,v),x_n) \approx f(f(v,u),x_n)$, and similarly for $y\theta_n$. Yet these unifiers are independent of each other, i.e. for any $m < n$, θ_m does not $C1$-subsume θ_n.

The problem is of course the overlap between the axioms (or the self-overlap of an axiom). However, at the other end of the spectrum, it was proved in [1] that unification modulo theories with *flat* leaf-permutative axioms (of depth 1, and without constant symbols), is finitary. Hence some amount of overlapping is admissible, as in the theory $S4$ defined by the two axioms

$$f(x,y,z,u) \approx f(y,x,z,u) \text{ and } f(x,y,z,u) \approx f(y,z,u,x);$$

which contains all identities $f(x,y,z,u) \approx f(x,y,z,u)\sigma$ for permutations σ of $\{x,y,z,u\}$. This is due to the fact that the two permutations $(x\ y)$ and $(x\ y\ z\ u)$ generate the whole symmetric group on $\{x,y,z,u\}$.

Our goal is to exploit this group-theoretic structure, by introducing *permutative rewriting* in Section 3 (here, *permutative* refers to the use of permutation groups). The rewriting system is represented concisely by a set $\mathcal{C}$ of linear terms and a function that to each of these terms associates a group of permutations of its variables.

However, all the terms congruent to the left-hand side of a leaf-permutative axiom may not be obtained by permutations of the variables, for instance the theory AC can be defined by two leaf-permutative axioms $f(x,y) \approx f(y,x)$ and $f(f(x,y),z) \approx f(f(y,z),x)$, which entail the axiom of associativity $f(f(x,y),z) \approx f(x,f(y,z))$, and this axiom is not leaf-permutative. We therefore define a condition of *unify-stability* on $\mathcal{C}$ that rules out this possibility, by ensuring that the underlying rewriting system is closed under critical pairs.

We then give in Section 4 a polynomial test on the set of axioms that is sufficient to ensure that a unify-stable set $\mathcal{C}$ exists, and can be computed. We are then able to define a unification algorithm in Section 5, with rather standard rules except for a *permutative decomposition* rule. These rules are proved correct and complete in Section 6. We finally prove in Section 7 that the algorithm terminates, and that it runs in simply exponential time. We first introduce the necessary notations.

2. Notations

We use notions and notations that are mostly standard to rewriting and unification, and can be found for instance in [2].

We are given an infinite set of variables $\mathcal{X}$, and a signature Σ of symbols, each with an *arity* $n \in \mathbb{N}$. *Function* symbols have a non-zero arity, *constants* have arity 0. The *head symbol* of the term $f(t_1, \ldots, t_n)$ is f.

A *position* is a finite sequence of integers; let $\mathcal{P}$ denote the set of positions (containing the empty sequence ε). If p is a position of t, denoted by $p \in \mathrm{Pos}(t)$, then $t|_p$ is a *subterm* of t. The *length* of t is $|t| = |\mathrm{Pos}(t)|$. The set of subterms of t which are variables is denoted by $\mathrm{Var}(t)$, and if $t|_p$ is a variable, we say that p is a *variable position* of t. We will use the metavariables c and e to denote linear terms.

We write $s \preccurlyeq t$ if s is a subterm of t, and $s \prec t$ for the corresponding strict order. We say that the positions p and q are *disjoint* if none is a prefix of the other, and then that $t|_p$ and $t|_q$ are *disjoint subterms* of t (they may still be comparable by $\preccurlyeq$). The term obtained from t by *replacement* of its subterm at position $p \in \mathrm{Pos}(t)$ by a term s is denoted by $t[s]_p$.

A *substitution* σ is a function from variables into terms, such that the set $\mathrm{Dom}(\sigma)$ (its *domain*) of non-fixpoints is finite. The unique substitution σ of domain $\{x_1, \ldots, x_n\}$ such that $\sigma(x_i) = t_i$ for all $i \in \{1, \ldots, n\}$ is denoted by $\sigma = \{x_1 \leftarrow t_1, \ldots, x_n \leftarrow t_n\}$. The *restriction* of σ to a set $X \subseteq \mathcal{X}$ is the substitution of domain $X \cap \mathrm{Dom}(\sigma)$ which is identical to σ on this domain. For any term t, we write $t\sigma$ for the term obtained from t by simultaneously substituting every variable x by the term $\sigma(x)$. We then say that $t\sigma$ is an *instance* of t. We will also apply substitutions σ to sets of terms by applying σ to all their elements.

The *range* $\mathrm{Rng}(\sigma)$ of σ is the image by σ of $\mathrm{Dom}(\sigma)$. If $\mathrm{Rng}(\sigma) \subset \mathcal{X}$, and σ is injective, we say that σ is a *variable renaming*, or simply a *renaming*. This of course implies that σ is a permutation of $\mathrm{Dom}(\sigma)$. The set of renamings whose domain is included in a set $X \subseteq \mathcal{X}$ will be identified with the symmetric group on X; its identity will be denoted by id. Two terms s and t (resp. substitutions μ and θ) are *variants* of each other, written $s \sim t$ (resp. $\mu \sim \theta$), if there is a variable renaming σ such that $s\sigma = t$ (resp. $\mu\sigma = \theta$). These are both equivalence relations.

An *identity*, or *equation*, is an ordered pair of terms, written $l \approx r$; l is its *left-hand side* and r its *right-hand side*. For a given set E of identities, the *rewriting* relation modulo E on terms is denoted by $\rightarrow_E$. We write $\approx_E$ for the *equational theory* induced by E; the elements of E are its *axioms*, and we will always assume that they do not share variables.

An *E-unification problem* S is a finite set of identities, denoted by

$$S = \{t_1 =^?_E t'_1, \ldots, t_n =^?_E t'_n\}.$$

We let $\mathrm{Var}(S) = \bigcup_{i=1}^{n} \mathrm{Var}(t_i) \cup \mathrm{Var}(t'_i)$. The set of E-unifiers of S is denoted by $\mathcal{U}_E(S)$. If t_i is a variable that has no other occurrence in S, it is *solved in* S. If every t_i is a variable x_i solved in S, we say that S is *in solved form*; it induces an E-unifier $\theta_S = \{x_i \leftarrow t'_i \mid 1 \leqslant i \leqslant n\}$. For any substitution σ, we let $S\sigma$ be the problem $\{t_1\sigma =^?_E t'_1\sigma, \ldots, t_n\sigma =^?_E t'_n\sigma\}$.

Given two substitutions θ, θ' and a set of variables $X \subseteq \mathcal{X}$, we say that θ *E-subsumes* θ' *on* X if there is a substitution δ such that $x\theta\delta \approx_E x\theta'$ for all $x \in X$. If X (resp. E) is omitted, that means $X = \mathcal{X}$ (resp. $E = \emptyset$). A set U of E-unifiers of S is *complete*, or is a *CSU* for S if every E-unifier of S is E-subsumed by an element of U on $\mathrm{Var}(S)$. If there is a CSU for S with only one element, this element is a *most general* E-unifier for S, or *mgu*.

We will also consider *first-order* unification problems, i.e. with $E = \emptyset$, and write $t =^? t'$ for $t =^?_\emptyset t'$. If the problem $\{t_1 =^? t_2, \ldots, t_1 =^? t_n\}$ has a unifier, we say that the terms $t_1, \ldots, t_n$ are *unifiable*. Then there is an mgu, which is unique up to $\sim$, and there always exists an idempotent mgu; one of these will be denoted by $\mathrm{mgu}(t_1, \ldots, t_n)$. Let γ be this mgu, the most general common instance $t_i\gamma$ will be denoted by $\sqcup\{t_1, \ldots, t_n\}$ (or $t_1 \sqcup t_2$ if $n = 2$).

3. Permutative rewriting

Definition 3.1. An equation is *leaf-permutative* if it has the form $c \approx c\sigma$, where c is linear and σ is a permutation of $\mathrm{Var}(c)$.

For any linear term c and set of axioms E, we let $\Gamma_E(c)$ be the set of permutations σ of $\mathrm{Var}(c)$ such that $c \approx_E c\sigma$.

In the sequel, we consider a set E of leaf-permutative axioms.

Definition 3.2. For any position $p \in \mathcal{P}$ and linear term c, we define on the set of terms the binary relation of *permutative rewriting* by: $t \rightarrowtail^p_c t'$ iff $p \in \mathrm{Pos}(t)$, there exists a substitution μ such that $c\mu = t|_p$ and there exists a permutation $\sigma \in \Gamma_E(c)$ such that $t' = t[c\sigma\mu]_p$. In other words, t rewrites into t' by applying an identity $c \approx c\sigma$ at position p (see Fig. 1). We will write $\leftarrowtail^p_c$ for the inverse of $\rightarrowtail^p_c$.

A set $\mathcal{C}$ of linear terms *covers* E if

(1) E is a logical consequence of the set $\{c \approx c\sigma \mid c \in \mathcal{C}, \sigma \in \Gamma_E(c)\}$,

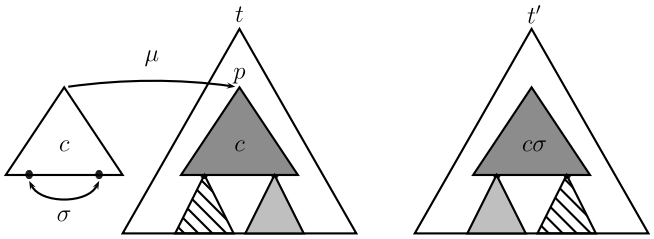

Fig. 1. The permutative rewriting relation $t \rightarrowtail^p_c t'$.

(2) for all $f \in \Sigma$ of arity $n > 0$, there is a *congruence term* $c_f = f(x_1, \ldots, x_n)$ in $\mathcal{C}$, where $x_1, \ldots, x_n$ are distinct variables,
(3) the terms in $\mathcal{C}$ do not share variables.

We let $\rightarrowtail_{\mathcal{C}}$ denote the relation $\bigcup_{c \in \mathcal{C}, p \in \mathcal{P}} \rightarrowtail_c^p$.

Obviously, the permutative rewriting relations are included in $\approx_E$. As a first consequence (which is not limited to leaf-permutative axioms) we have:

Theorem 3.3. *$\Gamma_E(c)$ is a group.*

Proof. For any $\sigma, \sigma' \in \Gamma_E(c)$, we obviously have $c \rightarrowtail_c^{\varepsilon} c\sigma$, and (with $\mu = \sigma$) we also have $c\sigma \rightarrowtail_c^{\varepsilon} c\sigma'\sigma$. By transitivity of $\approx_E$ we get $c \approx_E c\sigma'\sigma$, hence $\sigma'\sigma \in \Gamma_E(c)$, which shows that this is indeed a finite permutation group. □

For any given c and p, there are terms that do not match c at position p, hence that are not related to any term by $\rightarrowtail_c^p$. This shows that these relations are not reflexive. However:

Theorem 3.4. *The relations $\rightarrowtail_c^p$ are symmetric and transitive.*

Proof. If $t \rightarrowtail_c^p t' \rightarrowtail_c^p t''$, then there are substitutions μ, μ' and permutations $\sigma, \sigma' \in \Gamma_E(c)$ such that $c\mu = t|_p$, $t' = t[c\sigma\mu]_p$, $c\mu' = t'|_p = c\sigma\mu$ and $t'' = t[c\sigma'\mu']_p$. Since σ' is a permutation of $\mathrm{Var}(c)$, we must also have $c\sigma'\mu' = c\sigma'\sigma\mu$, and therefore $t'' = t[c\sigma'\sigma\mu]_p$. Since $\sigma'\sigma \in \Gamma_E(c)$, we get $t \rightarrowtail_c^p t''$.

If $t \rightarrowtail_c^p t'$, then there is a substitution μ and a permutation $\sigma \in \Gamma_E(c)$ such that $c\mu = t|_p$ and $t' = t[c\sigma\mu]_p$, thus $t'|_p = c\sigma\mu$ and $t = t'[c\mu]_p = t'[c\sigma^{-1}\sigma\mu]_p$. Since $\sigma^{-1} \in \Gamma_E(c)$, we have $t' \rightarrowtail_c^p t$. □

Of course, only symmetry is preserved under unions:

Corollary 3.5. *For any set $\mathcal{C}$ of linear terms the relation $\rightarrowtail_{\mathcal{C}}$ is symmetric.*

This obviously yields completeness of the reflexive-transitive closure of permutative rewriting.

Theorem 3.6. *If $\mathcal{C}$ covers E, then the relations $\approx_E$ and $\rightarrowtail_S^{\star}$ are identical.*

Proof. For $c \in \mathcal{C}$, consider the set of equations $R_c = \{c \approx c\sigma \mid \sigma \in \Gamma_E(c)\}$. These equations are true in E, hence $R = \bigcup_{c \in \mathcal{C}} R_c$ is a logical consequence of E. But $\mathcal{C}$ covers E, hence R and E are logically equivalent.

By Birkhoff's Theorem, the relation $\approx_E$ is therefore identical to $\leftrightarrow_R^{\star}$, the equivalence closure of rewriting modulo R. We obviously have $\rightarrow_{R_c} = \bigcup_{p \in \mathcal{P}} \rightarrowtail_c^p$, hence $\rightarrow_R$ is $\rightarrowtail_{\mathcal{C}}$. By Corollary 3.5, the relation $\leftrightarrow_R^{\star}$ is exactly $\rightarrowtail_{\mathcal{C}}^{\star}$. □

By making the positions of rewriting explicit, we are able to study local confluence first on the easy cases.

Lemma 3.7. *If p and p' are disjoint positions, then $\rightarrowtail_c^p$ and $\rightarrowtail_{c'}^{p'}$ have the commuting diamond property: if $u \leftarrowtail_c^p t \rightarrowtail_{c'}^{p'} u'$ then there exists a term t' such that $u \rightarrowtail_{c'}^{p'} t' \leftarrowtail_c^p u'$.*

This fact is well-known, as part of the proof of the Critical Pair Lemma (see [2, p. 136]), in the case where two rewriting rules are applied at non-overlapping positions. Together with symmetry, this means that two consecutive permutative rewriting steps at disjoint positions can be swapped: if we have $u \rightarrowtail_c^p t \rightarrowtail_{c'}^{p'} u'$ then there exists a term t' such that $u \rightarrowtail_{c'}^{p'} t' \rightarrowtail_c^p u'$.

Lemma 3.8. *If $u \leftarrowtail_c^p t \rightarrowtail_{c'}^{pqp'} u'$, where $c|_q$ is a variable, then there exists a term t' and a variable position q' of c such that $u \rightarrowtail_{c'}^{pq'p'} t' \leftarrowtail_c^p u'$.*

This is part of the proof of the Strong Confluence Lemma (see [2, p. 145]), for linear term rewriting systems, in case of a non-critical overlap. We use the additional hypothesis that, in the linear rewriting rules, no variable disappears.

In order to obtain similar results for critical overlaps, we will have to make assumptions on $\mathcal{C}$ and, indirectly, on E. Basically, the assumptions will state that $\mathcal{C}$ accounts for all critical pairs. This will be done by imposing that the considered permutations belong to groups of the following form:

Definition 3.9. For any substitution μ, we let $\mathrm{Aut}(\mu)$ be the set of permutations σ of $\mathcal{X}$ such that for all variables $x \in \mathcal{X}$ we have $\sigma(x)\mu \sim x\mu$.

Since any two variables are variants of each other, $\mathrm{Aut}(\mu)$ contains all permutations of $\mathcal{X} \setminus \mathrm{Dom}(\mu)$, and is therefore infinite (its elements are not necessarily substitutions, this is why we use the more general notation $\sigma(x)$ instead of $x\sigma$). For example, if $\mu = \{x \leftarrow a, y \leftarrow a, z \leftarrow x\}$, then $(x\ y)(z\ u\ v)$ belongs to $\mathrm{Aut}(\mu)$, but $(x\ z)$ does not. It is easy to show that $\mathrm{Aut}(\mu)$ is a group, and that $\mathrm{Aut}(\mu) = \mathrm{Aut}(\mu')$ whenever $\mu \sim \mu'$. We now give a central result concerning the forms of the critical pairs that can be generated by two leaf-permutative equations. This is illustrated in Fig. 2.

Theorem 3.10. *Consider two linear terms c, c', a position $p \in \mathrm{Pos}(c')$ and a substitution μ such that $c\mu = c'|_p$. For any permutation $\sigma \in \Gamma_E(c) \cap \mathrm{Aut}(\mu)$, there exists a permutation $\pi \in \Gamma_E(c')$ such that $c'[c\sigma\mu]_p = c'\pi$.*

Proof. For all variables x of c, we have $x\sigma\mu \sim x\mu$ (these are the subterms pictured in light gray in Fig. 2), hence there is a variable renaming π_x such that $x\mu\pi_x = x\sigma\mu$, with $\mathrm{Dom}(\pi_x) = \mathrm{Var}(x\mu)$ and $\mathrm{Rng}(\pi_x) = \mathrm{Var}(x\sigma\mu)$.

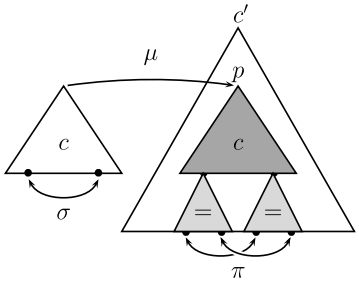

Fig. 2. Induced permutations.

Since the term c' is linear, the sets $\mathrm{Var}(x\mu)$ are disjoint for different variables x, and so are the sets $\mathrm{Var}(x\sigma\mu)$ (because σ is injective). We can then form the product π of the π_x's for all $x \in \mathrm{Var}(c)$, which is a permutation of $\bigcup_{x\in\mathrm{Var}(c)} \mathrm{Var}(x\mu) = \mathrm{Var}(c\mu) = \mathrm{Var}(c'|_p)$. Hence π is a permutation of $\mathrm{Var}(c')$.

We have $x\mu\pi = x\sigma\mu$ for all the variables of c, hence $c\mu\pi = c\sigma\mu$, so that

$$c'[c\sigma\mu]_p \;=\; c'[c\mu\pi]_p \;=\; c'[c\mu]_p\pi \;=\; c'\pi,$$

because all variables of c' which do not occur under position p are fixpoints of π. This proves that $c' \rightarrowtail^p_c c'\pi$, hence that $c' \approx_E c'\pi$, and finally that $\pi \in \Gamma_E(c')$. □

The critical pairs generated are therefore guaranteed to be leaf-permutative under the conditions given in Theorem 3.10. This leads to the following definition:

Definition 3.11. A set $\mathcal{C}$ of linear terms is *unify-stable* for E if it covers E and, for all $c, c' \in \mathcal{C}$,

(1) if c and c' are unifiable, then there is a $c'' \in \mathcal{C}$ and a substitution μ such that $c\mu = c'' \sim c \sqcup c'$ and $\Gamma_E(c) \subseteq \mathrm{Aut}(\mu)$,
(2) if there is a non-variable position $p \in \mathrm{Pos}(c)$ other than ε such that $c|_p$ and a variant of c' are unifiable, then there is a substitution μ such that $c'\mu = c|_p$ and $\Gamma_E(c') \subseteq \mathrm{Aut}(\mu)$.

Note that in the first item, c and c' can be swapped; if c and c' are unifiable, then c' and c are unifiable, and we must have $\Gamma_E(c') \subseteq \mathrm{Aut}(\mu')$, where $c'\mu' = c''$. The case $c = c'$ must also be considered, at least for the second item: this is why we have to consider a variant of c' (here, c) that may not share variables with $c|_p$, contrary to c. The first item is always true when $c = c'$, since μ is the identity, and $\mathrm{Aut}(\mathrm{id})$ contains every permutation of variables.

The two items of the definition lead respectively to the following two lemmas.

Lemma 3.12. *If $\mathcal{C}$ is unify-stable for E and $u \leftarrowtail^p_c t \rightarrowtail^p_{c'} u'$ with $c, c' \in \mathcal{C}$, then there is a $c'' \in \mathcal{C}$ such that $u \rightarrowtail^p_{c''} u'$.*

Proof. The subterm $t|_p$ is an instance of both c and c', which do not share variables or are identical, hence c and c' are unifiable, and there is a $c'' \in \mathcal{C}$ and a μ such that $c\mu = c'' \sim c \sqcup c'$. Hence c'' is a most general instance of c and c', and there must be a substitution ν such that $c''\nu = t|_p$. By $t \rightarrowtail^p_c u$ there exists a substitution μ' and a permutation $\sigma \in \Gamma_E(c)$ such that $c\mu' = t|_p$ and $u = t[c\sigma\mu']_p$.

Since $\mathcal{C}$ is unify-stable, we have $\Gamma_E(c) \subseteq \mathrm{Aut}(\mu)$, hence $\sigma \in \Gamma_E(c) \cap \mathrm{Aut}(\mu)$. We also have $c\mu = c''$, which is a linear term, hence by Theorem 3.10 there is a permutation $\pi \in \Gamma_E(c'')$ such that $c\sigma\mu = c''\pi$. We have $c\mu' = t|_p = c\mu\nu$, and since σ is a permutation of the variables of c, we must also have $c\sigma\mu' = c\sigma\mu\nu$. Hence obviously

$$u = t[c\sigma\mu']_p = t[c\sigma\mu\nu]_p = t[c''\pi\nu]_p,$$

and since $c''\nu = t|_p$, we get $t \rightarrowtail^p_{c''} u$.

Since u and u' play symmetric rôles in this proof, we also have $t \rightarrowtail^p_{c''} u'$. By Theorem 3.4 we get $u \rightarrowtail^p_{c''} u'$. □

Lemma 3.13. *If $\mathcal{C}$ is unify-stable for E and $u \leftarrowtail_c^p t \rightarrowtail_{c'}^{pq} u'$ where $q \neq \varepsilon$ is a non-variable position of c and $c, c' \in \mathcal{C}$, then $u \rightarrowtail_c^p u'$.*

Proof. There are substitutions ν and ν' such that $c\nu = t|_p$ and $c'\nu' = t|_{pq}$. Since q is a position in c, we have $(c|_q)\nu = (c\nu)|_q = t|_{pq} = c'\nu'$, hence $c|_q$ is unifiable with a variant of c'. Since $\mathcal{C}$ is unify-stable there is a substitution μ such that $c'\mu = c|_q$ and $\Gamma_E(c') \subseteq \mathrm{Aut}(\mu)$.

By $t \rightarrowtail_{c'}^{pq} u'$ there is a permutation $\sigma \in \Gamma_E(c')$ such that $u' = t[c'\sigma\nu']_{pq}$, and by Theorem 3.10 there is a permutation $\pi \in \Gamma_E(c)$ such that $c[c'\sigma\mu]_q = c\pi$. We have $c'\mu\nu = (c|_q)\nu = c'\nu'$, and since σ is a permutation of the variables of c', we must also have $c'\sigma\mu\nu = c'\sigma\nu'$; therefore $u' = t[c'\sigma\mu\nu]_{pq}$. But $t|_p = c\nu$, hence

$$u' \;=\; t[\,(c\nu)[\,c'\sigma\mu\nu\,]_q\,]_p \;=\; t[\,(c[\,c'\sigma\mu\,]_q)\,\nu\,]_p \;=\; t[\,(c\pi)\nu\,]_p,$$

which proves that $t \rightarrowtail_c^p u'$. By Theorem 3.4 we get $u \rightarrowtail_c^p u'$. □

It is then easy to see that the set of identities R given in the proof of Theorem 3.6 is closed under critical pairs, and we can thus use Theorem 3.1 from [18]:

Corollary 3.14. *If there is a finite set $\mathcal{C}$ unify-stable for E, then the E-unifiability problem is in **NP**, the E-unification problem is finitary, and the number of minimal unifiers is simply exponential.*

The BSM algorithm given in [16] can be used to solve such unification problems. However, this algorithm, aimed at a more general class of theories than the present one, has many sources of non-determinism, which we want to reduce in a simpler and more specialized algorithm. One important property for unification is that our theories are *syntactic* (see [15]). We actually prove the following stronger result:

Theorem 3.15. *If $\mathcal{C}$ is unify-stable for E and t, t' are terms that are not variables or constants, then $t \approx_E t'$ if and only if there exist a term $c \in \mathcal{C}$, a permutation $\sigma \in \Gamma_E(c)$ and substitutions μ, μ' such that $c\mu = t$, $c\mu' = t'$ and for every variable $x \in \mathrm{Var}(c)$, we have $x\sigma\mu \approx_E x\mu'$.*

Proof. The if part is trivial: since $x\sigma\mu \approx_E x\mu'$ is true for all variables of c, we have $c\sigma\mu \approx_E c\mu' = t'$, and of course $c\sigma \approx_E c$, so that $c\sigma\mu \approx_E c\mu = t$, and hence $t \approx_E t'$.

Suppose now that $t \approx_E t'$, then by Theorem 3.6 we have $t \rightarrowtail_{\mathcal{C}}^{\star} t'$. We first show that we can move any rewriting step at the root to the beginning of this sequence. Suppose there is a rewriting step at the root which is not the first in the sequence, then we have:

$$t \;\rightarrowtail_{\mathcal{C}}^{n}\; u \;\rightarrowtail_c^p\; v \;\rightarrowtail_{c'}^{\varepsilon}\; u' \;\rightarrowtail_{\mathcal{C}}^{\star}\; t',$$

with $n \geqslant 0$ and $c, c' \in \mathcal{C}$.

If $p = \varepsilon$, then by Lemma 3.12 $u \rightarrowtail_{c''}^{\varepsilon} u'$, with $c'' \in \mathcal{C}$. If $p \neq \varepsilon$ is a non-variable position of c', then by Theorem 3.4 we have $u' \leftarrowtail_{c'}^{\varepsilon} v \rightarrowtail_c^p u$. By Lemma 3.13 we get $u' \rightarrowtail_{c'}^{\varepsilon} u$, and therefore $u \rightarrowtail_{c'}^{\varepsilon} u'$. Otherwise, p must be of the form qp' where $c'|_q$ is a variable, and we have $u' \leftarrowtail_{c'}^{\varepsilon} v \rightarrowtail_c^{qp'} u$. By Lemma 3.8, there exists a term w and a position q' such that $u' \rightarrowtail_c^{q'p'} w \leftarrowtail_{c'}^{\varepsilon} u$. Therefore, $u \rightarrowtail_{c'}^{\varepsilon} w \rightarrowtail_c^{q'p'} u'$, and since $c'|_{q'}$ is a variable, $q'p' \neq \varepsilon$.

This shows that we can always reduce the length of a sequence of rewriting steps ending with a rewriting step at the root. By induction, we can find a term s, an element $c \in \mathcal{C}$ such that $t \rightarrowtail_c^{\varepsilon} s$, and

a sequence $s \rightarrowtail_{\mathcal{C}}^{\star} t'$ without rewriting steps at the root. If there is no rewriting step at the root in the original sequence, we take $s = t$ and c is the congruence term corresponding to the head symbol in t (and we rewrite with the permutation $\sigma = \mathrm{id}$).

We still have to get rid of rewriting steps in the sequence $s \rightarrowtail_{\mathcal{C}}^{\star} t'$ occurring at positions inside c. Suppose the first rewriting step at a non-variable position p of c is not the first in the sequence, then we have:

$$s \rightarrowtail_{\mathcal{C}}^{n} u \rightarrowtail_{c''}^{p'} v \rightarrowtail_{c'}^{p} u' \rightarrowtail_{\mathcal{C}}^{\star} t,$$

with $n \geqslant 0$ and $c', c'' \in \mathcal{C}$. Since p' is not a non-variable position in c, it cannot be a prefix of p.

If p and p' are disjoint positions, then by Lemma 3.7 there is a term w such that $u \rightarrowtail_{c'}^{p} w \rightarrowtail_{c''}^{p'} u'$. Otherwise, p must be a strict prefix of p', i.e. $p' = pq$ with $q \neq \varepsilon$. If q is a non-variable position in c', then by Lemma 3.13 we have $u \rightarrowtail_{c'}^{p} u'$. Otherwise, there must be a variable position q' in c' that is a prefix of q, hence $q = q'p''$. By Lemma 3.8 there is a variable position q'' of c' and a term w such that $u \rightarrowtail_{c'}^{p} w \rightarrowtail_{c''}^{pq''p''} u'$.

By induction we can thus obtain a sequence $t \rightarrowtail_{c}^{\varepsilon} s \rightarrowtail_{c'}^{p} s' \rightarrowtail_{\mathcal{C}}^{\star} t'$ whose length has not increased. Then, by Lemma 3.13, we get a sequence $t \rightarrowtail_{c}^{\varepsilon} s' \rightarrowtail_{\mathcal{C}}^{\star} t'$ whose length has strictly decreased. We can therefore reiterate this process, and converge to a sequence $t \rightarrowtail_{c}^{\varepsilon} s'' \rightarrowtail_{\mathcal{C}}^{\star} t'$ devoid of rewriting steps at non-variable positions of c.

Now we must have a substitution μ and a permutation $\sigma \in \Gamma_E(c)$ such that $t = c\mu$ and $s'' = c\sigma\mu$. Since $c\sigma\mu \rightarrowtail_{\mathcal{C}}^{\star} t'$ has no rewriting step inside c, t' must also be an instance of c, say $c\mu'$, and for all $x \in \mathrm{Var}(c)$ we have $x\sigma\mu \rightarrowtail_{\mathcal{C}}^{\star} x\mu'$. That is $x\sigma\mu \approx_E x\mu'$. □

4. Unify-stable axioms

Definition 3.11 provides a notion of unify-stability *for E* that is semantical: the property is invariant when the set of axioms E is replaced by an equivalent one, and in particular by the theory $\approx_E$. In the present section we will give a simpler, syntactic criterion for E (from [5]), which entails the semantic property.

Definition 4.1. A finite set of leaf-permutative axioms E is *unify-stable* if, for any two axioms $c \approx c\sigma$ and $c' \approx c'\sigma'$ in E, we have

(1) if c and c' are unifiable, then σ and σ' are in $\mathrm{Aut}(\mathrm{mgu}(c, c'))$,
(2) if there is a non-variable position p of c other than ε such that $c|_p$ and a variant of c' are unifiable, then there is a substitution μ such that $c'\mu = c|_p$ and $\sigma' \in \mathrm{Aut}(\mu)$.

We then consider, for any linear term e, the set $\mathrm{G}_E(e)$ of permutations π of $\mathrm{Var}(e)$ such that $e \rightarrow_E e\pi$.

Note that $\mathrm{G}_E(e) \subseteq \Gamma_E(e)$. The set $\mathrm{G}_E(e)$ is rather easy to compute, by trying to apply all axioms in E to all non-variable positions of e, and checking whether the result is an instance of e (and simultaneously computing π). This can be done in time linear in the length of e and in the length of E.

As an example let us consider the theory $C1$ given in the introduction; let $c = f(f(x, y), z)$, then the axiom of $C1$ is $c \approx c\ (x\ y)$. We consider the term $e = f(f(a, f(u, v)), b)$, then c matches e only at the root, which allows to swap a and $f(u, v)$, i.e. we have $e \approx_{C1} f(f(f(u, v), a), b)$. But this term is not an instance of e, and we therefore have $\mathrm{G}_{C1}(e) = \emptyset$.

However, we can then apply the axiom at position 1 in $f(f(f(u, v), a), b)$, yielding $f(f(f(v, u), a), b)$, and then again at position ε, yielding $f(f(a, f(v, u)), b)$, which is an instance of e. We thus obtain the equation $e \approx_{C1} e\ (u\ v)$, which proves that $(u\ v) \in \Gamma_{C1}(e)$, hence that $\Gamma_{C1}(e) = \{\mathrm{id}, (u\ v)\}$.

We see in this case that $\mathrm{G}_{C1}(e)$ is not a generating subset of the group $\Gamma_{C1}(e)$ (the smallest group containing $\emptyset$ is the trivial group $\{\mathrm{id}\}$). We will see later in this section that this is due to $C1$ not being unify-stable, which is easy to see: $c|_1$ is unifiable with a variant of c, but is (of course) not an instance of c.

More generally, it is easy to check whether a set of axioms E is unify-stable or not. The property $\sigma \in \mathrm{Aut}(\mu)$ is true when, for all variables x of c, the linear terms $x\mu$ and $x\sigma\mu$, with no common variable, are variants of each other. Unify-stability can be tested in time quadratic in the number of axioms, and linear in their length.

We now give an example of a unify-stable set of axioms:

$$g(x_1, x_2) \approx g(x_2, x_1), \tag{1}$$

$$f(y_1, y_2, y_3, y_4, a) \approx f(y_2, y_1, y_4, y_3, a), \tag{2}$$

$$f(g(z_1, z_2), g(z_3, z_4), z_5, z_6, z_7) \approx f(g(z_2, z_4), g(z_3, z_1), z_6, z_5, z_7). \tag{3}$$

Let $c \approx c\sigma$ denote axiom (2), and $c' \approx c'\sigma'$ denote axiom (3), i.e. we have $\sigma = (y_1\ y_2)(y_3\ y_4)$ and $\sigma' = (z_1\ z_2\ z_4)(z_5\ z_6)$. The linear terms c and c' are unifiable, with mgu

$$\gamma = \{y_1 \leftarrow g(z_1, z_2),\ y_2 \leftarrow g(z_3, z_4),\ y_3 \leftarrow z_5,\ y_4 \leftarrow z_6,\ z_7 \leftarrow a\}.$$

The elements of $\mathrm{Aut}(\gamma)$ are all the permutations π such that $\pi(z_7) = z_7$ and $\pi(\{y_1, y_2\}) = \{y_1, y_2\}$; it is clear that σ and σ' are both elements of this group.

Let $e \approx e\pi$ denote axiom (1), e is unifiable with $c'|_1$ and $c'|_2$, and is actually a variant of these two subterms. It is then obvious that condition (4.2) of Definition 4.1 holds, and therefore that this set of axioms is unify-stable.

In the remainder of this section we assume that E is unify-stable.

Definition 4.2. Let $\mathcal{E}$ be the set of linear terms obtained as most general instances of any number of left-hand sides of axioms in E, to which we add the congruence terms of Σ, in a way that no two terms in $\mathcal{E}$ share variables.

It is obvious that $\mathcal{E}$ covers E, and that $\mathcal{E}$ is closed under most general instances: if $e, e' \in \mathcal{E}$ are unifiable, then there is a $e'' \in \mathcal{E}$ such that $e'' \sim e \sqcup e'$ (if e is a congruence term, then $e'' = e'$). The property of unify-stability only involves the terms in E; our task is now to generalize it to the elements of $\mathcal{E}$. We first show how to preserve automorphisms of suitable substitutions.

Lemma 4.3. *If $C = \{c\mu_1, \ldots, c\mu_n\}$ is a unifiable set of linear terms with no common variables, and $c\mu = \sqcup C$, then $\bigcap_{i=1}^{n} \mathrm{Aut}(\mu_i) \subseteq \mathrm{Aut}(\mu)$.*

Proof. By induction on n. The case $n = 1$ is trivial. Suppose $n = 2$, and let $\sigma \in \mathrm{Aut}(\mu_1) \cap \mathrm{Aut}(\mu_2)$. Since the terms $c\mu_1$ and $c\mu_2$ are linear and do not share variables, we can decompose the unification problem $c\mu_1 =^? c\mu_2$ down to the variables x of c, and obtain:

$$\begin{aligned} x\mu &\sim x\mu_1 \sqcup x\mu_2 \\ &\sim \sigma(x)\mu_1 \sqcup x\mu_2 \text{ (since } \sigma(x)\mu_1 \sim x\mu_1 \text{ share no variable with } x\mu_2) \\ &\sim \sigma(x)\mu_1 \sqcup \sigma(x)\mu_2 \text{ (since } \sigma(x)\mu_2 \sim x\mu_2 \text{ share no variable with } \sigma(x)\mu_1) \\ &\sim \sigma(x)\mu, \end{aligned}$$

hence $\sigma \in \mathrm{Aut}(\mu)$.

We now suppose this is true for $C = \{c\mu_1, \ldots, c\mu_n\}$ and $c\mu = \sqcup C$ with $n \geqslant 2$, let $C' = C \cup \{c\mu_{n+1}\}$ and μ' be such that $c\mu' = \sqcup C' = c\mu \sqcup c\mu_{n+1}$. By what precedes we have

$$\bigcap_{i=1}^{n+1} \mathrm{Aut}(\mu_i) \subseteq \mathrm{Aut}(\mu) \cap \mathrm{Aut}(\mu_{n+1}) \subseteq \mathrm{Aut}(\mu'). \quad \square$$

We can now prove that, for any element e of $\mathcal{E}$, the permutations in $\mathrm{G}_E(e)$ account for all possible rewriting steps starting from e.

Lemma 4.4. *$\forall e \in \mathcal{E}$, if $e \to_E e'$ then there is a permutation $\pi \in \mathrm{G}_E(e)$ such that $e' = e\pi$.*

Proof. There is an axiom $c \approx c\sigma$ in E, a position p of e and a substitution μ such that $e|_p = c\mu$ and $e' = e[c\sigma\mu]_p$. Since $e \in \mathcal{E}$ there is a set C of unifiable left-hand sides of axioms of E, such that $e = \sqcup C$.

Let C' be the set of terms $c' \in C$ that have a non-variable position p. Since p cannot be a variable position of e, the set C' is not empty. Since the terms in C are linear and do not share variables, we have

$$c\mu = (\sqcup C)|_p \sim \sqcup\{c'|_p \mid c' \in C'\}.$$

Hence, for any $c' \in C'$, the term $c'|_p$ is unifiable with c (or a variant of c if $c' = c$ and $p \neq \varepsilon$). We now use the fact that E is unify-stable, and distinguish two cases.

- If $p = \varepsilon$, then for any mgu $\mu_{c'}$ of c and c' we have $\sigma \in \mathrm{Aut}(\mu_{c'})$. We choose the mgu's $\mu_{c'}$ so that the linear terms $c\mu_{c'}$ do not share variables, for different $c' \in C' = C$. We have

$$\sqcup\{c\mu_{c'} \mid c' \in C'\} = \sqcup\{c \sqcup c' \mid c' \in C\} \sim (\sqcup C) \sqcup c \sim c\mu.$$

- If $p \neq \varepsilon$, then there exists a substitution $\mu_{c'}$ such that $c\mu_{c'} = c'|_p$ and $\sigma \in \mathrm{Aut}(\mu_{c'})$. It is obvious that $\sqcup\{c\mu_{c'} \mid c' \in C'\} \sim c\mu$.

In both cases we are in position to apply Lemma 4.3, which yields $\sigma \in \mathrm{Aut}(\mu)$. Since $\sigma \in \Gamma_E(c)$, by Theorem 3.10 there exists a permutation π such that $e' = e[c\sigma\mu]_p = e\pi$. By definition we have $\pi \in \mathrm{G}_E(e)$. $\square$

We can now show that sequences of rewriting steps correspond to products of such admissible permutations. This requires some care, in particular because the set $G_E(e)$ is not preserved under permutations.

Lemma 4.5. *For any permutation σ of the variables of e, we have*

$$G_E(e\sigma) = \sigma^{-1} G_E(e)\sigma.$$

Proof. The relation $\to_E$ is stable under substitutions, hence

$$\pi \in G_E(e) \text{ iff } e \to_E e\pi \text{ iff } e\sigma \to_E e\pi\sigma \text{ iff } \sigma^{-1}\pi\sigma \in G_E(e\sigma). \qquad \square$$

This is enough for our purpose, since the σ's we will use are also products of admissible permutations.

Lemma 4.6. *$\forall e \in \mathcal{E}$, if $e \approx_E e'$ then there is a permutation π in the group G generated by $G_E(e)$, such that $e' = e\pi$.*

Proof. We have a sequence of rewriting steps

$$e = e_1 \leftrightarrow_E e_2 \leftrightarrow_E \cdots \leftrightarrow_E e_n = e'.$$

Suppose that $G_E(e_i) \subseteq G$, which is obvious for $i = 1$. If $e_i \to_E e_{i+1}$ then by Lemma 4.4 there is a permutation $\pi_i \in G_E(e_i)$ such that $e_{i+1} = e_i\pi_i$. Then $\pi_i \in G$, and by Lemma 4.5 we have $G_E(e_{i+1}) = \pi_i^{-1} G_E(e_i)\pi_i \subseteq G$.

If $e_{i+1} \to_E e_i$ there is a permutation $\pi \in G_E(e_{i+1})$ such that $e_i = e_{i+1}\pi$; we thus let $\pi_i = \pi^{-1}$, and we have $e_{i+1} = e_i\pi_i$. We also have $G_E(e_i) = \pi^{-1} G_E(e_{i+1})\pi$, hence $\pi = \pi^{-1}\pi\pi \in G_E(e_i)$, so that $\pi_i \in G$, and $G_E(e_{i+1}) \subseteq G$.

By induction we get $e' = e\pi_1 \cdots \pi_{n-1}$, and since each π_i is in G, so is their product. $\square$

This obviously has the following consequence:

Theorem 4.7. *$\forall e \in \mathcal{E}$, the group $\Gamma_E(e)$ is generated by $G_E(e)$.*

This means that we are able to compute a generating set for each group $\Gamma_E(e)$ in polynomial time. Generators provide very compact representations of permutation groups, as low as $O(n^2)$ where n is the number of variables of e, when of course the group $\Gamma_E(e)$ can have up to $n!$ elements. Suitable generating sets can be used to perform efficient computations on generated groups; this is the subject of *computational group theory*, see e.g. [13,7]. It is for instance easy from these generators to list all the elements of the group $\Gamma_E(c)$ without repetitions.

Another consequence of the previous lemma is that, using the identities $e \approx e\pi$ as rewriting rules inside other elements of $\mathcal{E}$ only results in permutations of their variables.

Lemma 4.8. *$\forall e, e' \in \mathcal{E}$, if we have a position p of e and a substitution μ such that $e|_p = e'\mu$, then $\Gamma_E(e') \subseteq \mathrm{Aut}(\mu)$.*

Proof. For any $\sigma \in \Gamma_E(e')$, we have $e' \approx_E e'\sigma$, hence $e \approx_E e[e'\sigma\mu]_p$. Since $e \in \mathcal{E}$, by Lemma 4.6 there is a permutation $\pi \in G_E(e)$ such that $e[e'\sigma\mu]_p = e\pi$. We therefore have $e'\sigma\mu = (e\pi)|_p = (e|_p)\pi =$

$e'\mu\pi$. This means that, for all variables x of e' we have $x\sigma\mu = x\mu\pi$, hence $x\sigma\mu \sim x\mu$. This proves that $\sigma \in \mathrm{Aut}(\mu)$. □

We can thus conclude that our syntactic criterion of unify-stability on sets of axioms E entails the existence of a unify-stable set for E, which is $\mathcal{E}$.

Theorem 4.9. *$\mathcal{E}$ is a unify-stable set for E.*

Proof. We already mentioned that $\mathcal{E}$ covers E. For all $e, e' \in \mathcal{E}$, we have sets C and C' of left-hand sides of axioms of E such that $e = \sqcup C$ and $e' = \sqcup C'$.

(1) If e and e' are unifiable, then there is a $e'' \in \mathcal{E}$ and a substitution μ such that $e\mu = e'' \sim e \sqcup e'$, hence by Lemma 4.8 we have $\Gamma_E(e) \subseteq \mathrm{Aut}(\mu)$.
(2) If there is a non-variable position p of e other than ε such that $e|_p$ is unifiable with a variant of e', then there is a non-empty set C'' of terms $c \in C$ that have a non-variable position p, and $e|_p \sim \sqcup\{c|_p \mid c \in C''\}$.
For any $c \in C''$, the term $c|_p$ is unifiable with a variant of $e' = \sqcup C'$, hence for any $c' \in C'$, $c|_p$ is unifiable with a variant of c', and must therefore be an instance of c' since E is unify-stable. Thus $c|_p$ is a common instance of the terms in C', hence is also an instance of their most general instance e'. Hence the common instance $e|_p$ of the terms $c|_p$ is also an instance of e'. Let μ be the substitution such that $e|_p = e'\mu$, by Lemma 4.8 we have $\Gamma_E(e') \subseteq \mathrm{Aut}(\mu)$. □

5. Transformation rules for unification

We now present the transformation rules that permit to solve any unification problem modulo a theory defined by a given set E of leaf-permutative axioms, a given finite unify-stable set $\mathcal{C}$ for E, and the groups $\Gamma_E(c)$ for all $c \in \mathcal{C}$. These rules are more elaborate than those presented in [6,8], where the notion of term graphs was used, i.e. a pointer structure for implementing terms. This was not suitable for the present paper because it requires a lengthy apparatus to be developed. Using the standard notion of terms is simpler (except for managing variables), but incurs a loss of information, hence of control of the transformation rules.

In particular, in order to recover the exponential upper bound on the number of unifiers from [8], it is now necessary to keep some extra information attached to unification problems. It is used to prevent useless applications of a costly (permutative) decomposition rule, and essentially represents equalities that are known to hold in a sense defined below.

Definition 5.1. Let D be an E-unification problem and t and t' be two terms. D is *consistent* with $t =^?_E t'$ if

- $\mathcal{U}_E(D) \subseteq \mathcal{U}_E\big(\{t =^?_E t'\}\big)$,
- for every $u =^?_E u'$ in D, either $u \prec t$ and $u' \prec t'$, or $u' \prec t$ and $u \prec t'$.

Let S be an E-unification problem, we say that a binary relation R on terms is *S-consistent* if for every $t\ R\ t'$, there exists a $D \subseteq S$ such that D is consistent with $t =^?_E t'$.

An *extended E-unification problem* (or EUP) is a finite multiset M of ordered pairs, written $S:R$, where S is an E-unification problem, and R is a binary relation on terms. We write $S:R$ for the singleton $\{S:R\}$. An EUP M is *consistent* if for all its elements $S:R$, R is S-consistent.

The set $\mathcal{U}_E(M)$ of E-unifiers of M is the union of the sets $\mathcal{U}_E(S)$ for all $S:R$ in M. We say that M is in *solved form* if for every $S:R$ in M, S is in solved form, hence induces an E-unifier θ_S; we then let $\Theta_M = \{\theta_S \mid S:R \in M\}$, and we obviously have $\Theta_M \subseteq \mathcal{U}_E(M)$.

One feature we need for solving an equation is the possibility to expand it according to the elements in $\mathcal{C}$. For example, consider a linear term $c = f(g(u,v),w)$, and the terms $t = f(x,a)$ and $t' = f(y,b)$, and suppose we want to solve the equation $t =^?_E t'$. If we are allowed to move w in c, for instance if $(v\ w) \in \Gamma_E(c)$, then a solution to the equation is $\{x \leftarrow g(z,a),\ y \leftarrow g(z,b)\}$. We must provide a means to introduce new symbols from c (here, g) and new variables in the original equation.

Definition 5.2. Given a linear term $c \in \mathcal{C}$, and two terms t and t', we consider two variable renamings μ_1 and μ_2 of $\mathrm{Var}(c)$ into "fresh" variables (i.e. variables that have not been used in the computation so far), and we consider the first-order unification problem $S = \{c\mu_1 =^? t,\ c\mu_2 =^? t'\}$; if it is solvable, we say that *t and t' are unifiable under c*, and we let $\gamma_c(t,t')$ be the idempotent mgu computed from S by the standard rules for first-order unification, with higher priority given to decomposition.[1]

In the sequel, when we use $\gamma_c(t,t')$ we may also use the corresponding μ_1 and μ_2 without explicitly defining them.

Following our example, if μ_1 (resp. μ_2) renames c's variables u,v,w into x_1,x_2,x_3 (resp. y_1,y_2,y_3), we get

$$\gamma_c(t,t') = \{x \leftarrow g(x_1,x_2),\ y \leftarrow g(y_1,y_2),\ x_3 \leftarrow a,\ y_3 \leftarrow b\}.$$

Once an expansion for a particular $c \in \mathcal{C}$ is considered, it is easy to see that we still have to consider all permutations in the group $\Gamma_E(c)$. Take for instance a unification problem $S = \{f(x_1,\ldots,x_n) =^?_E f(a_1,\ldots,a_n)\}$ where the a_i's are n distinct constants. Let $c_f = f(x_1,\ldots,x_n)$ and, for all $\sigma \in \Gamma_E(c_f)$, let $\theta_\sigma = \{\sigma(x_i) \leftarrow a_i \mid 1 \leqslant i \leqslant n\}$. Then θ_σ is an E-unifier of S, and these unifiers are not redundant: θ_σ is E-subsumed by $\theta_{\sigma'}$ only if $\sigma = \sigma'$. Hence the P-decomposition rule, defined below, needs to generate one new unification problem for every element of the group $\Gamma_E(c)$ (and for every $c \in \mathcal{C}$).

Definition 5.3. Consider an EUP $(\{t =^?_E t'\} \cup S):R$, where t and t' have the same head symbol, which is a function symbol (and not a constant). For any $c \in \mathcal{C}$,

- if t and t' are not unifiable under c, we define $\mathrm{D}(t,t',c,S,R) = \emptyset$,
- otherwise let $\gamma = \gamma_c(t,t')$, $X = (\mathrm{Var}(t) \cup \mathrm{Var}(t')) \cap \mathrm{Dom}(\gamma)$, and $R' = \{\langle t\gamma, t'\gamma\rangle\} \cup R\gamma$, we define $\mathrm{D}(t,t',c,S,R) = \{S^c_\sigma : R' \mid \sigma \in \Gamma_E(c)\}$ where for every $\sigma \in \Gamma_E(c)$,

$$S^c_\sigma \ = \ \{x\sigma\mu_1\gamma =^?_E x\mu_2\gamma \mid x \in \mathrm{Var}(c)\} \cup \{x =^?_E x\gamma \mid x \in X\} \cup S\gamma.$$

[1] Any reasonable implementation of unification works this way. This is only an optimization that minimizes the number of new variables introduced by our algorithm; it also makes some proofs simpler in Section 7.

trivial:

$$\frac{\{\{t =^?_E t'\} \cup S : R\} \cup M}{\{S : R\} \cup M} \text{ if } t = t' \text{ or } t\ R\ t'$$

orient:

$$\frac{\{\{t =^?_E x\} \cup S : R\} \cup M}{\{\{x =^?_E t\} \cup S : R\} \cup M} \text{ if } t \text{ is not a variable}$$

clash:

$$\frac{\{\{f(t_1, \ldots, t_n) =^?_E g(t'_1, \ldots, t'_m)\} \cup S : R\} \cup M}{M} \text{ if } f \neq g$$

occurrence test:

$$\frac{\{\{s =^?_E t\} \cup S : R\} \cup M}{M} \text{ if } s \text{ is a proper subterm of } t$$

replacement:

$$\frac{\{\{x =^?_E u\} \cup S : R\} \cup M}{\{\{x =^?_E u\} \cup S\{x \leftarrow u\} : R\{x \leftarrow u\}\} \cup M} \text{ if } x \in \mathrm{Var}(S) \setminus \mathrm{Var}(u)$$

P-decomposition:

$$\frac{\{\{t =^?_E t'\} \cup S : R\} \cup M}{[\bigcup_{c \in \mathcal{C}} \mathrm{D}(t, t', c, S, R)] \cup M} \text{ where } (i) \text{ and } (ii) \text{ hold}$$

(*i*) $t \neq t'$ and $t \not R\ t'$,
(*ii*) t and t' have the same head function symbol.

Fig. 3. The transformation rules.

If M, M' are extended unification problems, we write $M \to M'$ if M' derives from M by one of the rules given in Fig. 3.

The first group of equations in S^c_σ link subterms of $t'\gamma$ (on the right) and subterms of $t\gamma$ (on the left), to which we implicitly apply the rewriting rule $c \to c\sigma$. The second group of equations realizes the expansion required for applying this rewriting rule. The P-decomposition rule can thus be seen as a combination of narrowing and standard decomposition, with the obvious difference that we use a non-terminating rewriting system. Note that standard decomposition is encompassed by P-decomposition, since for all $f \in \Sigma$ we have $c_f \in \mathcal{C}$ (and of course $\mathrm{id} \in \Gamma_E(c_f)$).

Following our example, assuming that $\mathcal{C} = \{c, c_f, c_g\}$ and $\Gamma_E(c) = \{\mathrm{id}, (v\ w)\}$, $\Gamma_E(c_f) = \Gamma_E(c_g) = \{\mathrm{id}\}$; we attach to the unification problem $\{t =^?_E t'\}$ the empty relation, i.e. we take $R = \emptyset$. There are no remaining equations: we have $S = \emptyset$. Expanding with $c \in \mathcal{C}$, the corresponding γ exists, as above, and $X = \{x, y\}$. Obviously $R\gamma = \emptyset$, hence $R' = \{\langle f(g(x_1, x_2), a), f(g(y_1, y_2), b)\rangle\}$.

We compute S^c_σ for $\sigma = \mathrm{id}$ and $\sigma = (v\ w)$. Let $S' = \{x =^?_E x\gamma,\ y =^?_E y\gamma\} = \{x =^?_E g(x_1, x_2),\ y =^?_E g(y_1, y_2)\}$, we have

$$\begin{aligned} S^c_{\mathrm{id}} &= \{u\mu_1\gamma =^?_E u\mu_2\gamma,\ v\mu_1\gamma =^?_E v\mu_2\gamma,\ w\mu_1\gamma =^?_E w\mu_2\gamma\} \cup S' \\ &= \{x_1 =^?_E y_1,\ x_2 =^?_E y_2,\ a =^?_E b,\} \cup S', \end{aligned}$$

$$S^c_{(v\ w)} = \{u\mu_1\gamma =^?_E u\mu_2\gamma,\ w\mu_1\gamma =^?_E v\mu_2\gamma,\ v\mu_1\gamma =^?_E w\mu_2\gamma\} \cup S'$$
$$= \{x_1 =^?_E y_1,\ a =^?_E y_2,\ x_2 =^?_E b\} \cup S'.$$

We then have $\mathrm{D}(t,t',c,\emptyset,R) = \{S^c_{\mathrm{id}} : R',\ S^c_{(v\ w)} : R'\}$. We now consider the next element in $\mathcal{C}$: since t and t' are both instances of c_f, $\gamma_{c_f}(t,t')$ is the identity, and $X = \emptyset$. With R'' that only contains the relation $\langle f(x,a),\ f(y,b)\rangle$, and $S^{c_f}_{\mathrm{id}} = \{x =^?_E y,\ a =^?_E b\}$, we get $\mathrm{D}(t,t',c_f,\emptyset,R) = \{S^{c_f}_{\mathrm{id}} : R''\}$. The last element in $\mathcal{C}$ is c_g, but we have $\mathrm{D}(t,t',c_g,\emptyset,R) = \emptyset$. The P-decomposition rule therefore yields the EUP $\{S^c_{\mathrm{id}} : R',\ S^c_{(v\ w)} : R',\ S^{c_f}_{\mathrm{id}} : R''\}$. The first and last elements lead to clashes, while the second, through the orient and replacement rules, yields the following solved form:

$$\{x_1 =^?_E y_1,\ y_2 =^?_E a,\ x_2 =^?_E b,\ x =^?_E g(y_1,b),\ y =^?_E g(y_1,a)\} : R'.$$

In this algorithm, we will always start with an EUP $S:\emptyset$, so that the elements of R are only produced by the P-decomposition rule; hence for any $t\ R\ t'$, the terms t and t' have the same head function symbol. It is then easy to see that, at each step of the algorithm, the choice of the rule to apply is determined by the choice of the equation to be treated (if any rule applies). Apart from the choice of this equation, the only source of non-determinism is the P-decomposition rule. We are therefore very close to commutative unification, where the C-decompose rule (see e.g. [2, p. 232]) appears as a particular case of our rule. Since the C-decompose rule is known to generate redundant unifiers, similarly the CSUs we obtain by P-decomposition are generally not minimal.

6. Correction and completeness

We will now establish the logical properties of our algorithm.

Lemma 6.1. *If $M \to M'$ by the orient, clash, occurrence test or replacement rule, then $\mathcal{U}_E(M) = \mathcal{U}_E(M')$.*

Proof. This is standard for the orient and replacement rules (see e.g. [2,3]). It holds for the clash rule because all equations in E have the same head symbol on both sides, and it holds for the occurrence test because all members of any E-congruence class have the same length (since E is leaf-permutative). □

The results of Section 3 can easily be used to prove that P-decomposition is correct, i.e. that it preserves unifiers. Note that the side condition (i) of the rule is not needed to ensure this property.

Lemma 6.2. *If $M' = \{\{t =^?_E t'\} \cup S : R\} \cup M$ is an EUP, then*

$$\mathcal{U}_E\left(\left[\bigcup_{c\in\mathcal{C}} \mathrm{D}(t,t',c,S,R)\right] \cup M\right) \subseteq \mathcal{U}_E(M').$$

Proof. Let $S' = \{t =^?_E t'\} \cup S$. Since $\mathcal{U}_E(M') = \mathcal{U}_E(S') \cup \mathcal{U}_E(M)$, we only need to prove that for all $c \in \mathcal{C}$ such that t and t' are unifiable under c, we have $\mathcal{U}_E(\mathrm{D}(t,t',c,S,R)) \subseteq \mathcal{U}_E(S')$, hence that for all $\sigma \in \Gamma_E(c)$, we have $\mathcal{U}_E(S^c_\sigma) \subseteq \mathcal{U}_E(S')$.

Let $\gamma = \gamma_c(t,t')$, $X = (\mathrm{Var}(t) \cup \mathrm{Var}(t')) \cap \mathrm{Dom}(\gamma)$, and $\theta \in \mathcal{U}_E(S^c_\sigma)$. We first have, for every $x \in \mathrm{Var}(c)$, $x\sigma\mu_1\gamma\theta \approx_E x\mu_2\gamma\theta$, and since $c\mu_1$ and $c\mu_2$ are neither variables nor constants, by Theorem 3.15 we have $c\mu_1\gamma\theta \approx_E c\mu_2\gamma\theta$, hence $t\gamma\theta \approx_E t'\gamma\theta$. Next, for all $x \in X$, $x\theta \approx_E x\gamma\theta$; since the variables in $c\mu_1$ and $c\mu_2$ are fresh, for any term s appearing in S', $\mathrm{Var}(s) \cap \mathrm{Dom}(\gamma) \subseteq X$ and $s\theta \approx_E s\gamma\theta$. Hence, we have $t\theta \approx_E t\gamma\theta \approx_E t'\gamma\theta \approx_E t'\theta$, and $\theta \in \mathcal{U}_E(\{t =^?_E t'\})$. Finally, we also have $\theta \in \mathcal{U}_E(S\gamma)$, and therefore, for every equation $s =^?_E s'$ in S, $s\theta \approx_E s\gamma\theta \approx_E s'\gamma\theta \approx_E s'\theta$, so that $\theta \in \mathcal{U}_E(S)$. This proves that $\theta \in \mathcal{U}_E(S')$. □

Proving the correctness of the trivial rule obviously requires an additional hypothesis on the binary relation R; we show that a consistency requirement suffices. We first need a lemma on consistency.

Lemma 6.3. *Suppose D is consistent with $t =^?_E t'$, then*

1. *for every substitution δ, $D\delta$ is consistent with $t\delta =^?_E t'\delta$,*
2. *if $D' \cup \{t =^?_E t'\}$ is consistent with $s =^?_E s'$, then so is $D \cup D'$.*

Proof.

(1) Since $\mathcal{U}_E(D) \subseteq \mathcal{U}_E(t =^?_E t')$, it is obvious that $\mathcal{U}_E(D\delta) \subseteq \mathcal{U}_E(t\delta =^?_E t'\delta)$. The equations in $D\delta$ are of the form $u\delta =^?_E u'\delta$, where $u =^?_E u'$ belongs to D, so that either $u \prec t$ and $u' \prec t'$, hence $u\delta \prec t\delta$ and $u'\delta \prec t'\delta$, or $u' \prec t$ and $u \prec t'$, hence $u'\delta \prec t\delta$ and $u\delta \prec t'\delta$. This proves that $S\delta$ is consistent with $t\delta =^?_E t'\delta$.

(2) We have

$$\begin{aligned}\mathcal{U}_E(D \cup D') &= \mathcal{U}_E(D) \cap \mathcal{U}_E(D') \\ &\subseteq \mathcal{U}_E\left(t =^?_E t'\right) \cap \mathcal{U}_E(D') \\ &\subseteq \mathcal{U}_E\left(\{t =^?_E t'\} \cup D'\right) \subseteq \mathcal{U}_E\left(s =^?_E s'\right).\end{aligned}$$

Moreover, we have either $t \prec s$ and $t' \prec s'$, or $t' \prec s$ and $t \prec s'$. For all equations $u =^?_E u'$, we therefore have either $u \prec s$ and $u' \prec s'$, or $u' \prec s$ and $u \prec s'$. This is also true for the equations in D', by hypothesis, hence $D \cup D'$ is consistent with $s =^?_E s'$. □

We can now show that the trivial rule is correct, complete, and preserves consistency.

Lemma 6.4. *If $M' = \{\{t =^?_E t'\} \cup S : R\} \cup M$ is a consistent EUP, and $t = t'$ or $t\ R\ t'$, then $\mathcal{U}_E(M') = \mathcal{U}_E(\{S : R\} \cup M)$, and $\{S : R\} \cup M$ is consistent.*

Proof. Let $S' = \{t =^?_E t'\} \cup S$, if $t = t'$ it is obvious that the set $D = \emptyset$ is consistent with $t =^?_E t'$; otherwise $t\ R\ t'$, and there is a set $D \subseteq S'$ consistent with $t =^?_E t'$. This equation cannot be in D, hence $D \subseteq S$. In both cases we let $S'' = S \setminus D$, and we have

$$\mathcal{U}_E(S') = \mathcal{U}_E(D) \cap \mathcal{U}_E(S'') \cap \mathcal{U}_E\left(\{t =^?_E t'\}\right) = \mathcal{U}_E(D) \cap \mathcal{U}_E(S'') = \mathcal{U}_E(S),$$

hence $\mathcal{U}_E(M') = \mathcal{U}_E(S') \cup \mathcal{U}_E(M) = \mathcal{U}_E(S) \cup \mathcal{U}_E(M) = \mathcal{U}_E(\{S : R\} \cup M)$.

There remains to show that R is S-consistent: suppose $s\ R\ s'$, then by hypothesis there exists a $D' \subseteq S'$ consistent with $s =^?_E s'$. If $D' \subseteq S$ we are done, otherwise the equation $t =^?_E t'$ must belong to D', so we let $D'' = (D' \setminus \{t =^?_E t'\}) \cup D$; it is clearly included in S, and by Lemma 6.3 (2), it is also consistent with $s =^?_E s'$. □

Since consistency is required by the trivial rule, it must be preserved by all the rules.

Lemma 6.5. *If $M \to M'$ and M is consistent, then so is M'.*

Proof. We have already proved this result if M' derives from M by the trivial rule, and it is obvious for the clash rule and occurrence test.

For the orient rule, we have a relation R that is $(\{t =^?_E x\} \cup S)$-consistent, and we must prove that R is also $(\{x =^?_E t\} \cup S)$-consistent. Suppose $s\ R\ s'$, then there exists a $D \subseteq \{t =^?_E x\} \cup S$ which is consistent with $s =^?_E s'$. If $D \subseteq S$ we are done, otherwise the equation $t =^?_E x$ must be in D, and we let $D' = D \setminus \{t =^?_E x\} \cup \{x =^?_E t\}$, which is a subset of $\{x =^?_E t\} \cup S$; we have $\mathcal{U}_E(D') = \mathcal{U}_E(D)$, and obviously we have either $t \prec s$ and $x \prec s'$, or $x \prec s$ and $t \prec s'$, hence D' is consistent with $s =^?_E s'$.

For the replacement rule, we have to prove that, given $S' = \{x =^?_E u\} \cup S$ such that $x \in \mathrm{Var}(S) \setminus \mathrm{Var}(u)$ and an S'-consistent relation R, it is the case that $R\delta$ is S''-consistent, where $\delta = \{x \leftarrow u\}$ and $S'' = \{x =^?_E u\} \cup S\delta$. Consider s and s' such that $s\ R\ s'$ (i.e. $s\delta\ (R\delta)\ s'\delta$), and let $D \subseteq S'$ be a set consistent with $s =^?_E s'$; by Lemma 6.3 *(1)*, $D\delta$ is consistent with $s\delta =^?_E s'\delta$. If $x =^?_E u \notin D'$ then $D \subseteq S$, hence $D\delta \subseteq S''$ and we are done. Otherwise, the set $D' = D \setminus \{x =^?_E u\}$ is included in S, hence $D'\delta \subseteq S''$. Since $x\delta = u = u\delta$, we have $D\delta = D'\delta \cup \{u =^?_E u\}$, hence $\mathcal{U}_E(D'\delta) = \mathcal{U}_E(D\delta)$, and therefore $D'\delta \subseteq D\delta$ is also consistent with $s\delta =^?_E s'\delta$.

For the P-decomposition rule, given $S' = \{t =^?_E t'\} \cup S$ and an S'-consistent relation R, we need to prove that, for any linear term $c \in \mathcal{C}$ such that t and t' are unifiable under c, and for any $\sigma \in \Gamma_E(c)$, the relation R' from Definition 5.3 is S^c_σ-consistent. Let $\gamma = \gamma_c(t, t')$, $X = (\mathrm{Var}(t) \cup \mathrm{Var}(t')) \cap \mathrm{Dom}(\gamma)$; we have $t\gamma\ R'\ t'\gamma$, and we show that the set $D = \{x\sigma\mu_1\gamma =^?_E x\mu_2\gamma \mid x \in \mathrm{Var}(c)\}$ is consistent with $t\gamma =^?_E t'\gamma$. By definition $D \subseteq S^c_\sigma$, the terms appearing in D are obviously strict subterms of t and t', and by Theorem 3.15, for every $\theta \in \mathcal{U}_E(D)$ we have $t\gamma\theta = c\mu_1\gamma\theta \approx_E c\mu_2\gamma\theta = t'\gamma\theta$, it follows that $\mathcal{U}_E(D) \subseteq \mathcal{U}_E(\{t\gamma =^?_E t'\gamma\})$.

Let $s\ R\ s'$ (i.e. $s\gamma\ R'\ s'\gamma$), then by hypothesis there exists a $D' \subseteq S'$ that is consistent with $s =^?_E s'$, hence by Lemma 6.3 *(1)* $D'\gamma$ is consistent with $s\gamma =^?_E s'\gamma$. If $D' \subseteq S$ then $D'\gamma \subseteq S^c_\sigma$ and we are done. Otherwise, the set $D'' = (D'\gamma \setminus \{t\gamma =^?_E t'\gamma\}) \cup D$ must be included in S^c_σ, and since D is consistent with $t\gamma =^?_E t'\gamma$, by Lemma 6.3 *(2)* D'' is consistent with $s\gamma =^?_E s'\gamma$. □

We finally need a completeness result for P-decomposition.

Lemma 6.6. *Given an EUP $S' : R$ where $S' = \{t =^?_E t'\} \cup S$ such that t and t' have the same head function symbol, every E-unifier of S' is subsumed on* $\mathrm{Var}(S')$ *by an E-unifier of $M = \bigcup_{c \in \mathcal{C}} \mathrm{D}(t, t', c, S, R)$.*

Proof. Let $\theta \in \mathcal{U}_E(S')$, we have $t\theta \approx_E t'\theta$, and $t\theta, t'\theta$ are neither variables nor constants; we can apply Theorem 3.15, yielding a linear term $c \in \mathcal{C}$, a pair of substitutions μ, μ' such that $c\mu = t\theta$ and $c\mu' = t'\theta$, and a permutation $\sigma \in \Gamma_E(c)$ such that $\forall x \in \mathrm{Var}(c), x\sigma\mu \approx_E x\mu'$.

We consider the problem $\{c\mu_1 =^? t, c\mu_2 =^? t'\}$, where the variables in $Y = \mathrm{Var}(c\mu_1) \cup \mathrm{Var}(c\mu_2)$ are fresh w.r.t. S'. We may assume that $Y \cap \mathrm{Var}(t\theta) = \emptyset$; otherwise we replace θ by a suitable variant, which of course subsumes θ. Note that $\mathrm{Var}(t\theta) = \mathrm{Var}(t'\theta)$, since $t\theta \approx_E t'\theta$ and E is leaf-permutative.

Since μ_1 and μ_2 are renamings with disjoint ranges, there exists a substitution δ such that $c\mu_1\delta = c\mu$ and $c\mu_2\delta = c\mu'$. Let θ' be the substitution equal to θ on $\mathcal{X} \setminus Y$, and to δ on Y; by construction, θ' subsumes θ on $\mathrm{Var}(S')$ (which is disjoint from Y). Moreover, θ' is a unifier of $\{t =^? c\mu_1,\ t' =^? c\mu_2\}$, since $c\mu_1\theta' = c\mu_1\delta = c\mu = t\theta = t\theta'$, and similarly $c\mu_2\theta' = t'\theta'$. This proves that t and t' are unifiable under c, and that $S^c_\sigma \in M$. We now prove that $\theta' \in \mathcal{U}_E(S^c_\sigma)$.

Let $\gamma = \gamma_c(t, t')$, it is idempotent and subsumes θ', hence there is a substitution τ such that $\gamma\tau = \theta'$, and we have $\gamma\theta' = \gamma^2\tau = \theta'$. We thus have $c\mu_1\gamma\theta' = c\mu$ and $c\mu_2\gamma\theta' = c\mu'$, hence for all $x \in \mathrm{Var}(c)$, $x\sigma\mu_1\gamma\theta' = x\sigma\mu \approx_E x\mu' = x\mu_2\gamma\theta'$, which proves that θ' is a unifier of $\{x\sigma\mu_1\gamma =^?_E x\mu_2\gamma \mid x \in \mathrm{Var}(c)\}$. For every $x \in \mathrm{Var}(t) \cup \mathrm{Var}(t')$, we depending on have $x\theta' = x\gamma\theta'$, and also $S\gamma\theta' = S\theta' = S\theta$. Since $\theta \in \mathcal{U}_E(S)$, we deduce that $\theta' \in \mathcal{U}_E(S\gamma)$, hence $\theta' \in \mathcal{U}_E(S^c_\sigma)$. □

We can now conclude.

Theorem 6.7. *For any E-unification problem S, if $S{:}\emptyset \to^\star M$ and M is a $\to$-normal form, then M is in solved form, and Θ_M is a CSU for S.*

Proof. Suppose M is not in solved form, then it must contain an EUP $S{:}R$ such that S contains an equation $t =^?_E t'$ and t is not a variable solved in S. It is then easy to check that some rule applies. For instance, if t and t' are not variables and have the same head symbol; if it is a constant the trivial rule applies, and if it is a function symbol either the P-decomposition or the trivial rule applies depending on whether $t\ R\ t'$ or not.

Since M is a $\to$-normal form, this is impossible, hence M is in solved form, and it is easy to see that every unifier of M is subsumed by an element of Θ_M. The initial EUP $S{:}\emptyset$ is trivially consistent, hence by induction all EUP's in the derivation are consistent (by Lemma 6.5), and are correct and complete by Lemmas 6.1, 6.2, 6.4 and 6.6. We therefore have $\Theta_M \subseteq \mathcal{U}_E(M) \subseteq \mathcal{U}_E(S)$, and every E-unifier of S is subsumed on $\mathrm{Var}(S)$ by an element of $\mathcal{U}_E(M)$, hence by an element of Θ_M. □

There remains to be proved that a $\to$-normal form can always be reached by $\to^\star$, i.e. by applying a finite sequence of rules.

7. Termination and complexity

We now prove that the transformation rules we have introduced terminate on any extended unification problem M, and we determine an upper-bound on the cardinalities of the CSUs that are computed. We need some tools in order to track the non-variable positions of the terms involved in M.

Definition 7.1. Given a term t and a linear term $c \in \mathcal{C}$, we write $t \asymp c$ when t and c have a common instance, but t is not an instance of c. We consider the set of subterms of t that are not variables: $\mathrm{T}(t) = \{s \preccurlyeq t \mid s \notin \mathcal{X}\}$. For any unification problem S, and set of terms U, we define

$$\mathrm{T}(S) = \bigcup_{t =^?_E t' \in S} \mathrm{T}(t) \cup \mathrm{T}(t') \text{ and } \mathrm{T}(U) = \bigcup_{t \in U} \mathrm{T}(t),$$

$$\mathcal{N}(S) = (\mathrm{T}(S) \times \mathcal{C}) \cap \asymp \text{ and } \mathcal{N}(U) = (\mathrm{T}(U) \times \mathcal{C}) \cap \asymp .$$

For any substitution θ and subset N of some product $U \times \mathcal{C}$, we define $N\theta$ by applying θ only to the left coordinate, i.e. $N\theta = \{\langle t\theta, c\rangle \mid \langle t, c\rangle \in N\}$.

Intuitively, $\mathcal{N}(S)$ represents the set of subterms on which the application of the P-decomposition rule would introduce new symbols or variables. We will show that the applications of our transformation rules decrease their number. We first prove some easy properties.

Lemma 7.2. *For any $c \in \mathcal{C}$, substitution θ and problem S,*

(1) $\mathrm{T}(S\theta) = \mathrm{T}(S)\theta \cup \mathrm{T}(\mathrm{Var}(S)\theta)$,
(2) $(\mathrm{T}(S)\theta \times \mathcal{C}) \cap \not\asymp \subseteq \mathcal{N}(S)\theta$.

Proof.

(1) Let $s \in \mathrm{T}(S\theta)$, then either there is a subterm $s' \in \mathrm{T}(S)$ such that $s = s'\theta$, hence $s \in \mathrm{T}(S)\theta$, or there is a variable $x \in \mathrm{Var}(S)$ such that $s \in \mathrm{T}(x\theta)$. The reverse inclusion is trivial.
(2) For any $\langle t\theta, c\rangle \in (\mathrm{T}(S)\theta \times \mathcal{C}) \cap \not\asymp$, we have $t \in \mathrm{T}(t)$ and $t\theta \not\asymp c$. The instance common to $t\theta$ and c is also common to t and c, and t is not an instance of c, otherwise $t\theta$ would also be. Hence $t \not\asymp c$, so that $\langle t, c\rangle \in \mathcal{N}(S)$, and therefore $\langle t\theta, c\rangle \in \mathcal{N}(S)\theta$. □

We analyze how these sets are transformed by the replacement rule.

Lemma 7.3. *Given $S = \{x =^?_E u\} \cup S''$ and $S' = \{x =^?_E u\} \cup S''\delta$, where $x \in \mathrm{Var}(S) \setminus \mathrm{Var}(u)$ and $\delta = \{x \leftarrow u\}$, we have*

$$\mathrm{T}(S') = \mathrm{T}(S)\delta \text{ and } \mathcal{N}(S') \subseteq \mathcal{N}(S)\delta.$$

Proof. We have $\mathrm{T}(S) = \mathrm{T}(u) \cup \mathrm{T}(S'')$ and $\mathrm{T}(S') = \mathrm{T}(u) \cup \mathrm{T}(S''\delta) = \mathrm{T}(S''\delta)$ since $x\delta = u$ appears in $S''\delta$. We also have $\mathrm{T}(S''\delta) = \mathrm{T}(S'')\delta \cup \mathrm{T}(u)$ by Lemma 7.2 (1),and since $u\delta = u$, we have $\mathrm{T}(S') = \mathrm{T}(S''\delta) = (\mathrm{T}(S'') \cup \mathrm{T}(u))\delta = \mathrm{T}(S)\delta$. Using Lemma 7.2 (2),we deduce $\mathcal{N}(S') = (\mathrm{T}(S)\delta \times \mathcal{C}) \cap \not\asymp \subseteq \mathcal{N}(S)\delta$. □

We now start the analysis of the P-decomposition rule. In the previous section we only used the logical properties of $\gamma_c(t, t')$; we now use the special properties of the particular mgu we compute.

Lemma 7.4. *Given a linear term $c \in \mathcal{C}$ and two terms t, t' unifiable under c, let $\gamma = \gamma_c(t, t')$ and $X = (\mathrm{Var}(t) \cup \mathrm{Var}(t')) \cap \mathrm{Dom}(\gamma)$, we have $\sum_{x\in X} |x\gamma| \leqslant 2|c|$, and for all $x \in X$, every element of $\mathrm{T}(x\gamma)$ is an instance of an element of $\mathrm{T}(c) \setminus \{c\}$. Moreover, if t and t' are instances of c, then $X = \emptyset$.*

Proof. Let $S = \{c\mu_1 =^? t, c\mu_2 =^? t'\}$ and $Y = \mathrm{Var}(c\mu_1) \cup \mathrm{Var}(c\mu_2)$. We compute γ by first eagerly applying to S the standard decomposition rule, yielding S'. Let X' be the set of variables x such that there is an equation $s =^? x$ in S', where s is not a variable. If t and t' are instances of c, hence of $c\mu_1$ and $c\mu_2$ respectively, we have $X' = \emptyset$.

For all $x \in X'$, let S_x be the set of equations of S' whose right-hand side is x, and $S'' = S' \setminus \bigcup_{x\in X'} S_x$; the equations in S'' must be of the form $y =^? s$ where $y \in Y$ and s is a subterm of t or t'. The variables in the left-hand sides of the equations of S' are the elements of Y, which are fresh, hence they occur only once in S'. Thus S'' is in solved form, and the problems S_x do not share variables. Let γ_x be

the unifier obtained from S_x (by applying the rules for first-order unification), these substitutions commute, hence we may form their product $\prod_{x\in X'}\gamma_x$ by composing them in any order. It is then easy to see that $\gamma = \theta_{S''}\prod_{x\in X'}\gamma_x$. Since x is the only variable from t or t' in $\mathrm{Dom}(\gamma_x)$, and no such variable is in $\mathrm{Dom}(\theta_{S''})$, we have $X' = X$.

For any $x \in X$, we write $S_x = \{e_1 =^? x, \ldots, e_n =^? x\}$; the e_i's are strict subterms of $c\mu_1$ or $c\mu_2$, hence are linear and do not share variables. Solving the problem $\{e_1 =^? x, e_2 =^? x\}$ would give values to some variables in e_1, e_2, and a value e'_1 to x, which is a most general common instance of e_1 and e_2; it is easy to see that e'_1 is linear and $\mathrm{Pos}(e'_1) = \mathrm{Pos}(e_1) \cup \mathrm{Pos}(e_2)$. Moreover, every $s \in \mathrm{T}(e'_1)$ occurs at a non variable position in e_1 or e_2, hence is an instance of an element of $\mathrm{T}(e_1) \cup \mathrm{T}(e_2)$; the e_i's are variants of strict subterms of c, hence s is an instance of an element of $\mathrm{T}(c)$ other than c. We also have $\mathrm{Var}(e'_1) \subseteq \mathrm{Var}(e_1) \cup \mathrm{Var}(e_2)$, hence $e'_1, e_3, \ldots, e_n$ do not share variables, and we can easily propagate the property by induction up to $e'_{n-1} = x\gamma$; every element of $\mathrm{T}(x\gamma)$ is an instance of an element of $\mathrm{T}(c) \setminus \{c\}$, and $\mathrm{Pos}(x\gamma) = \bigcup_{i=1}^n \mathrm{Pos}(e_i)$. Thus $|x\gamma| \leqslant \sum_{i=1}^n |e_i|$.

Let $P_x = \{p \in \mathrm{Pos}(c) \mid t|_p = x\}$ and $P'_x = \{p \in \mathrm{Pos}(c) \mid t'|_p = x\}$; we obviously have $\{e_1, \ldots, e_n\} = \{c\mu_1|_p \mid p \in P_x\} \cup \{c\mu_2|_p \mid p \in P_x\}$, hence

$$|x\gamma| \;\leqslant\; \sum_{i=1}^{n} |e_i| \;\leqslant\; \sum_{p\in P_x} |c\mu_1|_p| + \sum_{p\in P'_x} |c\mu_2|_p| \;=\; \sum_{p\in P_x} |c|_p| + \sum_{p\in P'_x} |c|_p|.$$

The elements of $P = \bigcup_{x\in X} P_x$ are variable positions in t, hence are disjoint, and so are the elements of $P' = \bigcup_{x\in X} P'_x$. We therefore have

$$\sum_{x\in X} |x\gamma| \;\leqslant\; \sum_{p\in P} |c|_p| + \sum_{p\in P'} |c|_p| \;\leqslant\; 2|c|. \qquad \square$$

Note that the unify-stability hypothesis is essential in the following result.

Corollary 7.5. *Under the same conditions, we have* $\mathcal{N}(X\gamma) = \emptyset$.

Proof. Suppose there exists an element $\langle s, c'\rangle \in \mathcal{N}(X\gamma)$, then $s \lessdot c'$ and there is an $x \in X$ such that $s \in \mathrm{T}(x\gamma)$. By Lemma 7.4, s is an instance of an element of $\mathrm{T}(c) \setminus \{c\}$, hence of $c|_p$ for some non-variable position $p \neq \varepsilon$ of c. Since s and c' have a common instance, so do $c|_p$ and c'. But $\mathcal{C}$ is unify-stable for E, hence $c|_p$ (and s) must be an instance of c', contradicting $s \lessdot c'$. $\square$

We can now prove the main result concerning the P-decomposition rule.

Theorem 7.6. *For any linear term* $c \in \mathcal{C}$, *permutation* $\sigma \in \Gamma_E(c)$, *unification problem* $S' = \{t =^?_E t'\} \cup S$, *where* t *and* t' *are unifiable under* c, *we have*

$$\mathrm{T}(S'^c_\sigma) \;\subseteq\; \mathrm{T}(S')\gamma \cup \mathrm{T}(X\gamma) \;\text{ and }\; \mathcal{N}(S'^c_\sigma) \;\subseteq\; \mathcal{N}(S')\gamma,$$

where $\gamma = \gamma_c(t, t')$ *and* $X = (\mathrm{Var}(t) \cup \mathrm{Var}(t')) \cap \mathrm{Dom}(\gamma)$. *Furthermore, if* $t \lessdot c$ *or* $t' \lessdot c$, *then the second inclusion is strict.*

Proof. Let $D = \{x\sigma\mu_1\gamma =^?_E c\mu_2\gamma \mid x \in \mathrm{Var}(c)\}$, since $c\mu_1\gamma = t\gamma$ and $c\mu_2\gamma = t'\gamma$, we have $\mathrm{T}(D) \subseteq \mathrm{T}(t\gamma) \cup \mathrm{T}(t'\gamma) = (\mathrm{T}(t) \cup \mathrm{T}(t'))\gamma \cup \mathrm{T}(X\gamma)$ by Lemma 7.2 (1). Let $D' = \{x =^?_E x\gamma \mid x \in X\}$, we have $\mathrm{T}(D') = \mathrm{T}(X\gamma)$. Since $\mathrm{Var}(S) \cap \mathrm{Dom}(\gamma) \subseteq X$, by Lemma 7.2 (2) we have $\mathrm{T}(S\gamma) \subseteq \mathrm{T}(S)\gamma \cup \mathrm{T}(X\gamma)$. Therefore

$$\begin{aligned}\mathrm{T}(S^c_\sigma) &= \mathrm{T}(D) \cup \mathrm{T}(D') \cup \mathrm{T}(S\gamma)\\ &\subseteq (\mathrm{T}(t) \cup \mathrm{T}(t') \cup \mathrm{T}(S))\gamma \cup \mathrm{T}(X\gamma) = \mathrm{T}(S')\gamma \cup \mathrm{T}(X\gamma).\end{aligned}$$

Using Lemma 7.2 (2) and Corollary 7.5, we obtain

$$\begin{aligned}\mathcal{N}(S^c_\sigma) &\subseteq [(\mathrm{T}(S')\gamma \times \mathcal{C}) \cap \lessdot] \cup [(\mathrm{T}(X\gamma) \times \mathcal{C}) \cap \lessdot]\\ &\subseteq \mathcal{N}(S')\gamma \cup \mathcal{N}(X\gamma) = \mathcal{N}(S')\gamma.\end{aligned}$$

Suppose that, say, $t \lessdot c$, then obviously $\langle t, c\rangle \in \mathcal{N}(S')$, hence $\langle t\gamma, c\rangle \in \mathcal{N}(S')\gamma$. But $t\gamma \not\lessdot c$, since $t\gamma$ is an instance of c, hence $\langle t\gamma, c\rangle$ is not a member of $\mathcal{N}(S^c_\sigma)$, which is therefore different from $\mathcal{N}(S')\gamma$. □

7.1. Termination

We now adapt standard complexity measures that are used to prove the termination of unification algorithms. With these measures, we will prove that $\to$ terminates, and determine the cardinalities of the CSUs that are computed.

We start by associating some values to $\mathcal{C}$, and then to unification problems.

Definition 7.7. Let k be the cardinality of $\mathcal{C}$, g be the maximal cardinality of the groups $\Gamma_E(c)$ for $c \in \mathcal{C}$, and l be the maximal length of the terms $c \in \mathcal{C}$. To any EUP $S:R$ we associate the tuple $\mathrm{m}(S:R) = \langle m_0, m_1, m_2, m_3, m_4, m_5\rangle$, where:

- $m_0 = |\mathcal{N}(S)|$,
- $m_1 = |(\mathrm{T}(S) \times \mathrm{T}(S)) \setminus R|$,
- $m_2 = |\mathrm{T}(S)|$,
- m_3 is the number of variables in S that are not solved in S,
- m_4 is the cardinality of S,
- m_5 is the number of equations $t =^?_E x$ in S, where t is not a variable.

We then map each extended E-unification problem M to the multiset $\dot{M}$ of $\mathrm{m}(S:P)$ for all $S:P \in M$. The well-founded strict order $M < M'$ is then defined as $\dot{M} \ll \dot{M}'$, where $\ll$ is the multiset order based on the lexicographic order on tuples, as defined in [2, p. 22]. We recall that $A \gg B$ if B is obtained from A by removing a multiset X and adding a multiset Y, such that for any tuple $y \in Y$ there is a tuple $x \in X$ such that y is strictly smaller than x.

Lemma 7.8. *If* $\{S:R\} \cup M \to \{S':R'\} \cup M$ *by the trivial, orient or replacement rule, with* m_i *and* m'_i *referring respectively to* $\mathrm{m}(S:R)$ *and* $\mathrm{m}(S':R')$, *we have*

Rule	m'_0	m'_1	m'_2	m'_3	m'_4	m'_5
Trivial	$\leqslant m_0$	$\leqslant m_1$	$\leqslant m_2$	$\leqslant m_3$	$\leqslant m_4 - 1$	$\leqslant m_5$
Orient	$\leqslant m_0$	$\leqslant m_1$	$\leqslant m_2$	$\leqslant m_3$	$\leqslant m_4$	$\leqslant m_5 - 1$
Replacement	$\leqslant m_0$	$\leqslant m_1$	$\leqslant m_2$	$\leqslant m_3 - 1$	$\leqslant m_4$	$\leqslant m_4$

Proof. The last three columns can be considered as standard results (see for instance [2, p. 75]). The stated inequalities on m'_0, m'_1 and m'_2 are obvious for the orient rule, since $\mathrm{T}(S') = \mathrm{T}(S)$, hence $\mathcal{N}(S') = \mathcal{N}(S)$, and $R' = R$. For the trivial rule, we have $\mathrm{T}(S') \subseteq \mathrm{T}(S)$, hence $\mathcal{N}(S') \subseteq \mathcal{N}(S)$, and $R' = R$; the same inequalities hold.

For the replacement rule, by Lemma 7.3 we have $\mathrm{T}(S') = \mathrm{T}(S)\delta$, therefore $m'_2 = |\mathrm{T}(S)\delta| \leqslant |\mathrm{T}(S)| = m_2$, and $\mathcal{N}(S') \subseteq \mathcal{N}(S)\delta$, thus $m'_0 \leqslant m_0$. Moreover,

$$\mathrm{T}(S') \times \mathrm{T}(S') \setminus R' \;=\; (\mathrm{T}(S) \times \mathrm{T}(S))\delta \setminus R\delta \;\subseteq\; (\mathrm{T}(S) \times \mathrm{T}(S) \setminus R)\delta,$$

hence $m'_1 \leqslant |(\mathrm{T}(S) \times \mathrm{T}(S) \setminus R)\delta| \leqslant |\mathrm{T}(S) \times \mathrm{T}(S) \setminus R| = m_1$. □

Lemma 7.9. *Consider a linear term $c \in \mathcal{C}$, a binary relation R and a unification problem $S' = \{t =^?_E t'\} \cup S$, where t and t' are unifiable under c and $t \not R t'$. For any permutation $\sigma \in \Gamma_E(c)$, let S^c_σ and R' be as in Definition 5.3. With m_i and m'_i referring respectively to* $\mathrm{m}(S' : R)$ *and* $\mathrm{m}(S^c_\sigma : R')$, *we have $m'_4 \leqslant m_4 + 3l$ and $m'_5 \leqslant m_4 + l$, and depending on whether t and t' are both instances of c (case 1), or not (case 2), we have*

	m'_0	m'_1	m'_2	m'_3
Case 1	$\leqslant m_0$	$\leqslant m_1 - 1$	$\leqslant m_2$	$\leqslant m_3$
Case 2	$\leqslant m_0 - 1$	$\leqslant m_1 + 4l(m_2 + l)$	$\leqslant m_2 + 2l$	$\leqslant m_3 + 2l$

Proof. Let $\gamma = \gamma_c(t, t')$ and $X = (\mathrm{Var}(t) \cup \mathrm{Var}(t')) \cap \mathrm{Dom}(\gamma)$, we have $S^c_\sigma = D \cup D' \cup S\gamma$, where as previously $D = \{x\sigma\mu_1\gamma =^?_E x\mu_2\gamma \mid x \in \mathrm{Var}(c)\}$ and $D' = \{x =^?_E x\gamma \mid x \in X\}$. By Theorem 7.6, $m'_0 = |\mathcal{N}(S^c_\sigma)| \leqslant |\mathcal{N}(S')| = m_0$, and if $t \prec c$ or $t' \prec c$, i.e. if we are in case 2, then the inequality is strict, so that $m'_0 \leqslant m_0 - 1$. Still by Theorem 7.6, $\mathrm{T}(S^c_\sigma) \subseteq \mathrm{T}(S')\gamma \cup \mathrm{T}(X\gamma)$, and therefore $m'_2 \leqslant |\mathrm{T}(S')\gamma| + |\mathrm{T}(X\gamma)| \leqslant m_2 + |\mathrm{T}(X\gamma)|$.

The number of equations in D is less than l, the number of equations in $S\gamma$ is less than m_4 (the cardinality of S'), and the $|X|$ equations in D' do not contribute to m'_5, hence $m'_4 \leqslant m_4 + l + |X|$ and $m'_5 \leqslant m_4 + l$. We obviously have $|X| \leqslant \sum_{x \in X} |x\gamma| \leqslant 2|c| \leqslant 2l$ by Lemma 7.4, hence $m'_4 \leqslant m_4 + 3l$.

The variables in $\mathrm{Var}(t) \cup \mathrm{Var}(t')$ are obviously unsolved in S', hence all variables solved in S' are fixpoints of γ, and are therefore solved in $S\gamma$, and thus also in S^c_σ (they do not occur in $D \cup D'$). Since we add in D' at most $2l$ variables (from $c\mu_i$), we have $m'_3 \leqslant m_3 + 2l$.

In case 2, by Lemma 7.4, $|\mathrm{T}(X\gamma)| \leqslant \sum_{x \in X} |x\gamma| \leqslant 2l$, hence $m'_2 \leqslant m_2 + 2l$. Considering the set $A = (\mathrm{T}(S')\gamma \times \mathrm{T}(X\gamma)) \cup (\mathrm{T}(X\gamma) \times \mathrm{T}(S')\gamma) \cup (\mathrm{T}(X\gamma) \times \mathrm{T}(X\gamma))$, we have

$$\begin{aligned}
\mathrm{T}(S^c_\sigma) \times \mathrm{T}(S^c_\sigma) \setminus R' \;&\subseteq\; \mathrm{T}(S^c_\sigma) \times \mathrm{T}(S^c_\sigma) \setminus R\gamma \\
&\subseteq\; [(\mathrm{T}(S') \times \mathrm{T}(S'))\gamma \cup A] \setminus R\gamma \\
&\subseteq\; (\mathrm{T}(S') \times \mathrm{T}(S') \setminus R)\gamma \cup A,
\end{aligned}$$

hence $m'_1 \leqslant m_1 + |A| \leqslant m_1 + 4l(m_2 + l)$.

In case 1, by Lemma 7.4 we have $X = \emptyset$, hence $D' = \emptyset$, so that $m'_3 \leqslant m_3$. We also have $\mathrm{T}(X\gamma) = \emptyset$, hence $m'_2 \leqslant m_2$, and

$$\begin{aligned}\mathrm{T}(S^c_\sigma) \times \mathrm{T}(S^c_\sigma) \setminus R' &\subseteq (\mathrm{T}(S') \times \mathrm{T}(S'))\gamma \setminus (R\gamma \cup \langle t\gamma, t'\gamma\rangle)\\ &\subseteq (\mathrm{T}(S') \times \mathrm{T}(S') \setminus R)\gamma \setminus \{\langle t, t'\rangle\gamma\}.\end{aligned}$$

Thus $\langle t, t'\rangle\gamma \notin \mathrm{T}(S^c_\sigma) \times \mathrm{T}(S^c_\sigma) \setminus R'$, and since $\langle t, t'\rangle \notin R$, we obviously have $\langle t, t'\rangle\gamma \in (\mathrm{T}(S') \times \mathrm{T}(S') \setminus R)\gamma$, hence $\mathrm{T}(S^c_\sigma) \times \mathrm{T}(S^c_\sigma) \setminus R' \subsetneq (\mathrm{T}(S') \times \mathrm{T}(S') \setminus R)\gamma$, and therefore $m'_1 < |(\mathrm{T}(S') \times \mathrm{T}(S') \setminus R)\gamma| \leqslant m_1$. □

We can deduce that:

Theorem 7.10. *The relation $\rightarrow$ terminates.*

Proof. We prove that if $M \rightarrow M'$, then $M' \prec M$. The result is obvious for the clash and occurrence test rules, since $M' \subsetneq M$. Lemma 7.8 proves the result for the trivial, orient and replacement rules, and Lemma 7.9 proves the result for the P-decomposition rule. □

7.2. Complexity

We are now going to determine an upper-bound on the number of transformation rules that can be applied to an EUP $S : R$. We will then prove that the cardinalities of the CSUs determined by our transformation rules have a simply exponential upper-bound, and that we can solve any unifiability problem in nondeterministic polynomial time.

Definition 7.11. Given a tuple $m = \langle m_0, m_1, m_3, m_4, m_5\rangle$, we denote by $\mathrm{M}(m)$ the maximal number of transformation rules that can be applied starting from any EUP $S : R$ such that $\mathrm{m}(S : R) = m$.

Theorem 7.12. *Given m as in Definition 7.11, let*

$$\begin{aligned}A_m &= m_0(1 + 4l(m_0 l + m_2)) + m_1 \text{ and}\\ B_m &= 3lm_3 + (2l + 1)m_4 + A_m l(12l + 3) + 6l + 1,\end{aligned}$$

we have $\mathrm{M}(m) \leqslant A_m B_m + m_3(1 + m_4) + m_4 + m_5$.

Proof. We prove the result by well-founded induction on the tuples m, using Lemmas 7.8 and 7.9. Suppose the result is true for every tuple $m' \prec m$, let $S' = \{t =^?_E t'\} \cup S$, and suppose that $\mathrm{m}(S' : R) = m$. We consider the different rules that can be applied to $S' : R$.

- If P-decomposition is applied, we have $\langle t, t'\rangle \in \mathrm{T}(S') \times \mathrm{T}(S') \setminus R$, thus $m_1 \geqslant 1$ and $A_m \geqslant 1$. Let $m' = \mathrm{m}(S^c_\sigma : R')$, by Lemma 7.9 we have $m'_3 \leqslant m_3 + 2l$, $m'_4 \leqslant m_4 + 3l$, $m'_5 \leqslant m_4 + l$, and it is simple to verify that $A_{m'} \leqslant A_m - 1$, regardless of whether t and t' are instances of c or not. We then have:

$$\begin{aligned}B_{m'} &\leqslant 3l(m_3 + 2l) + (2l + 1)(m_4 + 3l)\\ &\quad + (A_m - 1)l(12l + 3) + 6l + 1\end{aligned}$$

$$\leqslant B_m + 6l^2 + 3l(2l+1) - l(12l+3) = B_m$$

By the induction hypothesis we have:

$$\begin{aligned}
\mathrm{M}(m) &\leqslant 1 + \mathrm{M}(m') \\
&\leqslant 1 + A_{m'}B_{m'} + m'_3(1+m'_4) + m'_4 + m'_5 \\
&\leqslant 1 + (A_m - 1)B_m \\
&\quad +(m_3 + 2l)(1 + m_4 + 3l) + m_4 + 3l + m_4 + l \\
&\leqslant A_m B_m + m_3(1+m_4) + m_4 \\
&\quad +1 - B_m + 3lm_3 + 2l(m_4+1) + 6l^2 + m_4 + 4l \\
&\leqslant A_m B_m + m_3(1+m_4) + m_4 - 3A_m l - 6(2A_m - 1)l^2 \\
&\leqslant A_m B_m + m_3(1+m_4) + m_4 + m_5 \text{ (since } 2A_m \geqslant 1).
\end{aligned}$$

- Suppose the replacement rule is applied, then t is a variable x, let $\delta = \{x \leftarrow t'\}$, and $m' = \mathrm{m}(\{x =^?_E t'\} \cup S\delta : R\delta)$, by Lemma 7.8 we have $A_m \leqslant A_{m'}$, $m'_3 \leqslant m_3 - 1$, $m'_4 \leqslant m_4$, $m'_5 \leqslant m_4$, hence $B_{m'} \leqslant B_m$, and by the induction hypothesis we have:

$$\begin{aligned}
\mathrm{M}(m) &\leqslant 1 + A_m B_m + (m_3 - 1)(1 + m_4) + m_4 + m_4 \\
&\leqslant A_m B_m + m_3(1+m_4) + m_4 \\
&\leqslant A_m B_m + m_3(1+m_4) + m_4 + m_5.
\end{aligned}$$

- The result is trivial for all other rules. □

Given an initial unification problem S of length n, if $m = \mathrm{m}(S:\emptyset)$, then the cardinality m_0 of $\mathcal{N}(S)$ is at most $n|\mathcal{C}| = nk$, obviously m_2, m_3, m_4 and m_5 are bounded by n, and $m_1 \leqslant n^2$. We easily deduce:

Corollary 7.13. *Given a unification problem S of length n, the maximal length of one branch in the derivation tree starting from $\{S:\emptyset\}$ is bounded in $O(k^2 l^4 n^4)$.*

Since the P-decomposition rule generates at most kg new problems to solve, another trivial consequence is the following simply exponential bound:

Corollary 7.14. *Under the same conditions, the cardinality of the computed CSU is bounded in $O((kg)^{k^2 l^4 n^4})$.*

It should be noted that, due to the replacement rule, the length of the unification problems generated in our algorithm can increase exponentially. We now show that their size is polynomial if common subterms are shared.

Theorem 7.15. *The problem of solving an input unification problem S w.r.t. an input set of axioms E, and given an input unify-stable set $\mathcal{C}$ for E, is **NP**-complete.*

Proof. **NP**-hardness comes from that of commutative unification (see [12]); obviously if $E = \{f(x,y) \approx f(y,x)\}$, then $\mathcal{C} = \{f(x,y)\}$ is a unify-stable set for E.

We now show that we can guess a branch in the derivation tree starting from $S_0 : \emptyset$, and check that it is successful in time polynomial in the length of the input $S_0, E, \mathcal{C}$. We represent a branch by adding necessary information for proof-checking: the equation on which a rule is applied, and for the P-decomposition rule, the $c \in \mathcal{C}$ and the permutation σ that are used to compute S^c_σ. Moreover, we use maximal sharing of subterms to represent each node $S : R$. Let n be the length of S_0, and k, l be as in Definition 7.7.

By Corollary 7.13, the number of nodes on the branch is polynomial. The size required to represent each node can only increase when the P-decomposition rule is applied; so suppose it is applied to a node $(\{t =^?_E t'\} \cup S) : R$, yielding a node $S^c_\sigma : R'$. Since $R' = R \cup \{\langle t, t' \rangle\}$, the size of R' is less than the size of the node $(\{t =^?_E t'\} \cup S) : R$. The size of S^c_σ is $|\mathrm{T}(S^c_\sigma)| + |\mathrm{Var}(S^c_\sigma)|$; by Lemma 7.9 the cardinality of $\mathrm{T}(S^c_\sigma)$ can increase by at most $2l$ compared to that of $\mathrm{T}(S)$, and the number of variables can increase by at most $2l$ (the new variables come from $c\mu_1$ and $c\mu_2$). Hence the size of the node $S^c_\sigma : R'$ can increase by at most $4l$ compared to the parent node. In all cases the size of the nodes increase linearly in the length of the branch and in l, and is therefore polynomial.

Proof-checking can thus be performed in polynomial time; the only difficult point is to check, at any P-decomposition step, that for the specified c and σ we do have $\sigma \in \Gamma_E(c)$. We have seen in Theorem 4.7 that generators for this group can be computed, and this can be done in time polynomial in the lengths of E and c. From these generators it is possible to test membership of σ in the group $\Gamma_E(c)$ in polynomial time (see [11]). □

Note that the result does not hold if $\mathcal{C}$ is not an input to the problem, because its cardinality k can increase exponentially in the size of E (it is easy to find an example realizing this possibility). The E-unification decision problem, where E and therefore $\mathcal{C}$ are fixed, trivially belongs to **NP**.

8. Conclusion

In this paper, we introduced the unify-stability condition on the presentation of a leaf-permutative theory. This condition allows us to enforce a simple reduction strategy on permutative rewriting, which we used to define a set of transformation rules permitting to solve unification problems modulo theories with unify-stable presentations. These transformation rules are fairly intuitive and simpler than those of [16]. Furthermore, the unify-stability hypothesis is crucial in the proof of their termination. We also determined a simply exponential upper-bound on the CSUs computed by these rules, and showed that they can be used to test unifiability modulo the considered theory in nondeterministic polynomial time.

The efficiency of this algorithm depends on the set $\mathcal{C}$, which is not fixed for a given theory E. Indeed, E may have different unify-stable presentations, leading to sets $\mathcal{C}$ of different cardinalities, length of the elements $c \in \mathcal{C}$ or groups $\Gamma_E(c)$, and hence may have different impact on the efficiency. It may also be the case that, depending on the unification problem considered in the P-decomposition rule, some terms $c \in \mathcal{C}$ or some permutations $\sigma \in \Gamma_E(c)$ are necessarily redundant with others, and may thus be pruned. Such optimizations are certainly necessary to turn our transformation rules into a reasonably efficient algorithm.

Acknowledgments

We thank the anonymous referees for their careful reading and detailed comments.

References

[1] J. Avenhaus, Efficient algorithms for computing modulo permutation theories, in: David Basin, Michaël Rusinowitch (Eds.), Second International Joint Conference on Automated Reasoning, IJCAR 2004, Lecture Notes in Artificial Intelligence 3097, Springer Verlag, Cork, Ireland, 2004, pp. 430–444.
[2] F. Baader, T. Nipkow, Term Rewriting and All That, Cambridge University Press, Cambridge, 1998.
[3] F. Baader, W. Snyder, Unification theory, in: in: A. Robinson, A. Voronkov (Eds.), Handbook of Automated Reasoning, vol. 1, Elsevier, 2001, pp. 445–533.
[4] Franz Baader, Unification in commutative theories, Hilbert's basis theorem and Gröbner bases, Journal of the ACM 40 (3) (1993) 477–503.
[5] Thierry Boy de la Tour, Mnacho Echenim, Overlapping leaf permutative equations, in: David Basin, Michaël Rusinowitch (Eds.), Second International Joint Conference on Automated Reasoning, IJCAR 2004, Lecture Notes in Artificial Intelligence 3097, Springer Verlag, Cork, Ireland, 2004, pp. 430–444.
[6] Thierry Boy de la Tour, Mnacho Echenim, Unification in a class of permutative theories, in: Jürgen Giesl (Ed.), Sixteenth International Conference on Rewriting Techniques and Applications, RTA 2005, Lecture Notes in Computer Science 3467, Springer Verlag, Nara, Japan, 2005, pp. 105–119.
[7] G. Butler, Fundamental algorithms for permutation groups, in: Lecture Notes in Computer Science 559, Springer Verlag, 1991.
[8] Mnacho Echenim. Déduction et Unification dans les Théories Permutatives. Ph.D. thesis, Institut National Polytechnique de Grenoble, december 2005.
[9] François Fages, Associative-commutative unification, Journal of Symbolic Computation3 (1987) 257–275.
[10] Albrecht Fortenbacher, An algebraic approach to unification under associativity and commutativity, Journal of Symbolic Computation 3 (3) (1987) 217–229.
[11] M. Furst, J. Hopcroft, E. Luks. Polynomial time algorithms for permutation groups, in: Proceedings Twenty-first Annual Symposium on the Foundations of Computer Science, October 1980, pp. 36–41.
[12] M. Garey, D.S. Johnson, Computers and Intractability: a Guide to the Theory of **NP**-Completeness, Freeman, San Francisco, California, 1979.
[13] C. Hoffmann, Group-theoretic algorithms and graph isomorphism, in: Lecture Notes in Computer Science 136, Springer Verlag, 1981.
[14] Jean-Pierre Jouannaud, A set of eleven important open problems in term rewriting based theorem proving, Bulletin of the EATCS 31 (1987) 272–273.
[15] C. Kirchner, F. Klay, Syntactic theories and unification, in: John Mitchell (Ed.), Proceedings of the Fifth Annual IEEE Symposium on Logic in Computer Science, LICS 1990, IEEE Computer Society Press, 1990, pp. 270–277.
[16] Christopher Lynch, Barbara Morawska, Basic syntactic mutation, in: Andrei Voronkov (Ed.), CADE-18, Eighteenth International Conference on Automated Deduction, Lecture Notes in Computer Science, vol. 2392, Springer, 2002, pp. 471–485.
[17] Paliath Narendran, Friedrich Otto, Single versus simultaneous equational unification and equational unification for variable-permuting theories, Journal of Automated Reasoning 19 (1) (1997) 87–115.
[18] Robert Nieuwenhuis, Decidability and complexity analysis by basic paramodulation, Information and Computation 147 (1) (1998) 1–21.
[19] Manfred Schmidt-Schauß, Solution to problems p140 and p141, Bulletin of the EATCS 34 (1988) 274–275.
[20] Manfred Schmidt-Schauß, Unification in permutative equational theories is undecidable, Journal of Symbolic Computation 8 (4) (1989) 415–421.
[21] M.E. Stickel, A unification algorithm for associative-commutative functions, Journal of the Association for Computing Machinery 28 (1981) 423–434.